2022

K-12 EdTech Safety Benchmark: National Findings - Part 1

December 13, 2022

INTERNET SAFETY LABS

Acknowledgements

This document is an output from a project funded by the Internet Society Foundation.

Contributors

Andrea Ausland - Design
Alyssa Bernardino – Research
Daniella Doern – Research
Zach Edwards - Research
Irene Knapp – Research, Writing
Lisa LeVasseur – Research, Writing
Bryce Simpson – Research & Quantitative Analysis
Steven Turnbull – Research & Quantitative Analysis
George Vo – Quantitative Analysis

2022 K12 Edtech Safety Benchmark: National Findings – Part 1

1 Table of Contents

2 Executive Summary

This K12 Edtech Safety Benchmark report, the first of four, contains findings from an extensive, rigorous, and statistically significant research project that provides a deep look at children's edtech safety across U.S. schools.

The findings are disturbing. They clearly show personal information safety risks to children and families are present and pervasive in the technology recommended and used by U.S. educational institutions, including:

- Nearly all apps (96%) share children's personal information with third parties, 78% of the time with advertising and monetization entities, typically without the knowledge or consent of the users or the schools, making them unsafe
- 28% of apps were Non-Education Specific, such as The New York Times, YouTube or Spotify, effectively providing no limits or guardrails for children
- School apps (23%) expose kids to digital ads, which creates a risk that personal student data is being sent into advertising networks, with no way for the public to inspect where it goes or how it's used; more than half of those apps (13%) use retargeting ads, which use cookies, search and site history to serve up targeted advertising; this means even more personal student data is being sent into advertising networks to better serve the advertisers
- Google dominates K12 edtech as the prime supplier of both hardware and software, raising questions about the safety of having children deeply connected to the internet by the world's leading advertising platform

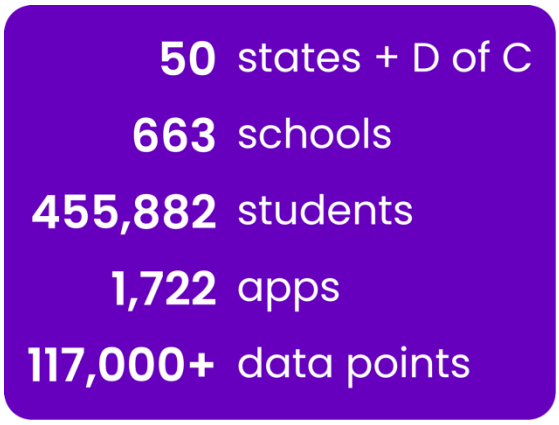
These and other research findings are summarized below and further developed throughout the report.

The research was conducted by the Internet Safety Labs (ISL, previously the Me2B Alliance), an organization dedicated to independent software product safety testing.

The safety benchmark validates and expands findings published by the ISL in its "School Mobile Apps Student Data Sharing Behavior" research (Spotlight Report #1, May 2021). That seminal study led to this massive project using actual analysis of apps and network traffic to examine in depth the broader question of what kind of safety risks exist across all K12 Edtech apps, especially in apps that are mandatory for students.

2.1 Scope

This benchmark evaluated K12 technology used in a random sampling of 13 schools in each of the 50 states and the District of Columbia, 663 schools in total, covering about 455,882 students.



In that sample, 1,722 apps (technologies) were either recommended or required by at least one school as indicated by the school and/or the district website. Internet Safety Labs tested 1,357 of those apps, collecting over 88,000 data points on the apps (including capturing network traffic for the apps) and over 29,000 data points on the schools.

This national summary findings report is the first of four reports on this substantial dataset.

The purpose of this research is to provide a baseline safety measurement of technology commonly used by K12 schools, which can be repeated every 3-5 years to evaluate safety trends.

2.2 Key Findings

2.2.1 Most apps used by K12 students are unsafe for children

Apps and technology that expose personal information about children and their families to technology providers, third-party marketers, advertisers and often the internet at large are not adequately safe for children.

At a minimum, it fuels marketers' and data brokers' personal data profiles ultimately used to bombard young minds with highly targeted and persuasive advertising or opinions. At worst, in the wrong hands it can lead to emotional trauma, aberrant seduction or even physical danger with location information.

Further, data is forever. For instance, mental health information gleaned from a child's innocent use of a mental health tracker can become a problem in later years as a teen or an adult.

To help establish guidelines for child-safe technology, the ISL developed a rigorous safety scoring rubric to evaluate K12 edtech apps.

The ISL scoring method evaluates many factors, including extensive and automated data gathering and sharing routines often buried deep inside app software components, as well as the observed network data sharing traffic to third parties.

Under the evaluation rubric, Do Not Use apps are judged too dangerous for use by students and High Risk means data is being shared with high-risk entities.

Based on the data analysis and ISL scoring, edtech apps were found overwhelmingly unsafe for use by students.

- **78%** of apps were scored **Do Not Use** and **18% High Risk**, meaning **96% of edtech apps are unsafe for students**.
- **74.9%** of all apps included one or more **Very High Risk** internal software component, known as SDKs, likely to share data with high-risk entities.
- **79%** of apps access **location** information based on permission analysis.
- **52%** of apps access **calendar** and **contacts** information.
- Of the top 25 **recommended** apps, **72%** were scored **Do Not Use** and **8%** were **High Risk**.
- Of the top 25 **mandatory** apps, **56%** were scored **Do Not Use, 20%** were scored **High Risk** and the remainder were untested.

2.2.2 Custom apps for school districts (aka school utility apps) are among the least safe apps

One might reasonably expect that mobile apps commissioned by school districts for use by students, parents, and teachers would be safe for kids. On the contrary, we found these apps to be among the least safe. The situation is made even more problematic given that these apps are promoted by the schools, such that we tagged them as "mandatory or key" for students.

- No Custom app received our safest score of Some Risk, and 89% of Custom apps were rated Do Not Use.
- Compared to Generic apps, Custom apps accessed Location Information and Social Information (address book, calendar) more, with 81% of Custom apps accessing Location information, and 69% of Custom apps accessing Social Information.
- Custom apps had more traffic to Facebook, Amazon and Twitter than generic apps.
- 61% of Custom apps were observed sending data to Google, significantly higher than the 49% of apps as reported in Spotlight Report #1.

2.2.3 School-recommended tech isn't strictly Edtech, nor is it strictly kid tech

There is much new regulatory activity relating to child-safe software design, which hinges on the notion that some technology is for kids and some is not. This boundary is much more liquid than current thinking allows. 28% of the apps recommended or

required by schools would not meet any proposed criteria to be classified as strictly for kids and therefore would not be subject to any child-safe design requirements.

- In total, 481 or 28% of the apps recommended or required by schools were not designed for use by children.
- 49% of the of apps recommended or required by schools were Non-Education Specific (NES) at 28% and [Edtech] Other (O) at 21%.
- The non-education specific apps include news publishers like The New York Times, music platforms like Spotify, donation service organizers like Bloomerang, and magazine e-readers like Flipster.
- Edtech Other includes educational games, health apps, and general productivity apps, among others.
- 85% of the NES apps were not designed for use by children, whereas 81% of the O apps were designed for use by children.

2.2.4 Edtech contains digital advertising

Digital advertising is inherently risky for people, never mind children, due to the potential for staggering information sharing. Retargeting (i.e., personalized) ads expose even more personal student data into the ad networks, which is why it is expressly prohibited in California's SOPIPA (Student Online Personal Information Protection Act), and several other state laws modeled after California's SOPIPA.

- 23% of apps recommended or required by schools included ads.
- 13% of apps recommended or required by schools included retargeting ads.

2.2.5 Google dominates K12 edtech in the US

With a primarily advertising-based business model and a vast and complicated business, Google's presence in US K12 schools through Google-produced hardware and software is deeply worrisome.

- **75%** of schools that provide personal computing devices to students are providing **Chrome OS based devices** (Chromebooks or Chrome tablets).
    - Devices based on **Apple** OSes were the next closest with only **34%**.
- **68%** of apps were observed sending data to **Google**.
    - This aligns also with the fact that **70%** of all apps included **Google SDKs**.
        - **56.9%** of **iOS** apps included **Google SDKs**; whereas **Android** apps never include **Apple** SDKs.
    - **Apple** was the second most heavily trafficked platform with **36%** of apps sending data to Apple. (Similarly, **38%** of apps included **Apple** SDKs.)
- Google developed the most apps in the top 25 mandatory/key apps with five (5) apps.

- Google Classroom was the second most required app with 27% of all schools requiring it.
    - PowerSchool Mobile was the most required app with 28% of schools requiring it.
- The Google Firebase analytics SDK was the most frequently used SDK across all apps; 67% of all apps with SDKs used Firebase.
- The top 5 SDKs used across all apps were Google SDKs.

2.2.6 82% of schools provide personal computing devices

As expected, most schools (82%) provide personal computing devices to students. This means schools need to have much more robust IT, cybersecurity and overall technology support capabilities in order to keep students safe while using technology.

2.2.7 Which are safer: Android or iOS apps?

In our earlier research (Spotlight Report #1), it seemed that iOS apps were appreciably safer than Android apps based on SDK risk. However, the results of this benchmark suggest that the difference in inherent safety of the two platforms is more complicated. Apps can be made safe — or unsafe — for people on either platform. However, Android apps do appear to be less safe overall than iOS apps. This bears further investigation.

- Safety scores were nearly the same across both OSes, but Android apps held a slight advantage.
    - 5% of Android apps had only Some Risk, compared to 3% of iOS apps.
    - 76% of Android apps were rated Do Not Use compared to 80% of iOS apps.
- However, based on SDKs, Android apps continue to be riskier:
    - On average, **Android** apps Include **nearly 3 times as many Very High-Risk SDKs** than **iOS** apps, **6.5** compared to **2.4**.
    - **iOS** apps were more often found to have zero (0) SDKs than Android apps with **68%** of the apps with no SDKs being iOS app.
    - **89.9%** of **Android** apps included **Very High Risk** SDKs as compared to **63.6%** of **iOS** apps
- **100%** of **Android** apps requested **Location** permissions**.**
- **iOS** apps more frequently **sent data** to all **six** large **platforms** than **Android** apps**.**
- **62%** of the safest apps were **iOS** apps**.**
- **80%** of the least safe apps were **Android** apps.

2.2.8 Recommending Technologies to Students: More Isn't Better

Several schools in our sample (40%) provided lengthy lists of recommended technologies for students with an average of 125 technologies listed per school. Interestingly, this number increased for schools that seemed to be doing some kind of vetting of technologies (26% of schools), to 172 technologies per school.

Schools are no doubt trying to be helpful to students by recommended technology, but in this case, given the poor scores of apps in this research, more isn't better.

- For schools/districts that had aggregated lists of recommended technologies, the average number of technologies was a staggering **125** technologies.
- For schools/districts that provided lists of approved technologies, the average number of technologies listed was an even more jaw-dropping **172** technologies.
- We found one school with a list of approved technologies topping out at **1,411**.

2.3 Wrapping Up – toward a safer Internet

Internet Safety Labs, a 501(c)(3) non-profit, is on a mission to correct the long-standing omission of product safety testing for software driven products. ISL is an independent software product safety organization. Our mission is to ensure safety in connected products and services through safety standards, product research, product safety audits and policy advocacy. We safety test every physical product in our lives and it's time we do the same with software.

While this K12 Edtech Safety Benchmark report and the research data we have compiled may seem discouraging, it is our hope that it will stir a broader awakening to the real safety risks present in the internet and the technology we use with it. It is also important to note that this work establishes a *baseline* measurement, and is the first of its kind in providing a large-scale, independent software product safety audit.

It's often said that the first step to dealing with a problem is recognizing there *is* a problem. This benchmark provides a clear indication of where improvement is needed and Internet Safety Labs is here to help developers and LEAs help keep students safe.

Throughout 2023 we will continue to share more data and findings from this pivotal 2022 K12 Edtech Safety Benchmark.

For more information and to follow our ongoing progress, please visit the Internet Safety Labs website.

3 Glossary

3.1 Advertising

In this report, we use the term Advertising to mean digital advertising of any sort.

3.2 K12

K12 is shorthand for kindergarten through twelfth grade, the full range of primary education for children in the US.

3.3 Contextual Advertising

Contextual advertising refers to digital advertising content based on characteristics of the publication site, not based on characteristics of the individual (i.e. not personalized).

3.4 Custom Apps (aka School Utility Apps)

For this research, we use two broad distinguishing categories for mobile apps: Custom and Generic. Custom apps are mobile apps that have been commissioned by a local education entity (i.e. either a school, a district, or a state-level entity) and are customized. In Spotlight Report #1, we referred to these apps as School Utility apps. In this research, we refer to them as Custom Apps.

These apps are often provided by large edtech platform manufacturers like Blackboard and Apptegy. The apps are essentially skin-able versions of the same app, used by hundreds of schools. These apps can appear in app stores with the developer listed as the platform manufacturer *or* the LEA who commissioned the custom app. We will probe this further in a future report.

3.5 Edtech

Edtech is the collection of digital technologies (app, webservices, etc.) that are used in an educational capacity, whether in schools (primary, secondary, post-secondary, adult education, etc.), or for individual, personal educational and enrichment purposes.

3.6 Edtech App Category

Edtech apps come in a very wide range of functionality and utility. We created an edtech typology to compare like-to-like edtech apps. The categories are listed here and details on the typology can be found in Appendix A.

- **Classroom Messaging Software (CMS)**
- **Community Engagement Platform (CEP)**
- **Digital Learning Platform (DLP)**

- **Learning Management System (LeMS)**
- **Library Management Software (LiMS)**
- **Non-Education Specific (NES)**
- **[Educational] Other (O)**
- **School Transportation Software (STS)**
- **Safety Platform (SP)**
- **Single Sign On (SSO)**
- **School Management Software (SMS)**
- **Student Information System (SIS)**
- **Study Tools (ST)**
- **Virtual Classroom Software (VCS)**

3.7 Generic Apps

Generic apps are mobile apps that are available off the shelf (OTS) to local educational agencies, parents, students, teachers, etc. These apps are typically not customized.

3.8 Local Educational Agency

"Local educational agency or LEA means a public board of education or other public authority legally constituted within a State for either administrative control or direction of, or to perform a service function for, public elementary schools or secondary schools in a city, county, township, school district, or other political subdivision of a State, or for a combination of school districts or counties as are recognized in a State as an administrative agency for its public elementary schools or secondary schools." https://sites.ed.gov/idea/regs/c/a/303.23

For the purposes of this research, a school, a school district, a state school board, or any combination of the above can comprise a local educational agency.

3.9 Permission Categories

We classified iOS and Android sensitive permissions into seven Permission Categories:

- **Location** includes any permission that potentially allows apps to determine the user's geographic location. Permissions such as wifi network names and bluetooth connections are included in this category because in many cases these names are distinctive and can be compared against databases to guess the location.
- **Files** include any permission that allows apps to list user data files or their contents, whether in the cloud or on device. This access is risky both because files and filenames can include personal information and because it can be

used to fingerprint and reidentify a user even if they have reset other identifiers.

- **Join User Identifiers** includes any permission that directly assists advertising networks that wish to track users across apps or across device, such as with Apple's ID for Advertising (IDFA).
- **Physical Environment** includes permissions that reveal information about the user's physical environment, such as through camera and microphone.
- **User Behavior** permissions include anything that would be useful to advertising networks seeking to learn more about a user, such as their psychology or interests.
- **Crash Logs** include permissions that allow the app publisher to receive information when the app crashes. There is a risk of this information including personal details.
- **Social Information** includes permissions that reveal who the user associates with, as well as when or where they do so. This includes calendar and contacts.
- **Phone Service** includes permissions that reveal who the user's carrier is or whether they currently have service. This can serve as a proxy for location. It may also reveal financial wellbeing.

3.10 Retargeting Advertising

For this research, retargeting advertising is digital advertising based on the user's browsing history.

3.11 School Utility Apps (aka Custom Apps)

See Custom Apps.

3.12 Software Developer Kit (SDK)

From our Spotlight Report #1:

> "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."

4 Introduction to the Benchmark

In May of 2021, Internet Safety Labs (ISL, previously Me2B Alliance) published research evaluating the behavior of a small set of K12 "school utility apps". School utility apps are all-purpose communication apps that are typically custom apps or school-branded [white-labeled] apps. The findings of that research were disturbing and prompted the broader question of what kind of safety risks exist across all K12 Edtech apps, especially apps that are mandatory for students?

This current research performs a more rigorous and statistically significant scale of technology auditing and provides a look at edtech safety across US schools.

Throughout 2022, ISL has been collecting data on a sample of 13 schools in every state in the US plus the District of Columbia. In the process, we have assembled a sizable database of both school/district behaviors relating to digital technology, as well as a database of over 1700 apps that schools/districts are recommending or requiring students to use.

4.1 Benchmark Reports

Due to the very large volume of data in this nearly year-long research project, we are releasing the results in a series of reports.

The current plan for reports is as follows (subject to change):

1. 2022 Edtech Safety Benchmark: National Findings (Part 1) [this report].
2. 2022 Edtech Safety Benchmark: State Findings – state summaries for all 50 states.
3. 2022 Edtech Safety Benchmark: National Findings (Part 2) – including state and regional comparisons, and nationwide demographic analysis.
4. 2022 Edtech Safety Benchmark: Regulatory and Technology Vetting Impacts – school and district technology vetting, notice and consent practices across the US, as well as third-party certification analysis.

4.2 What the Benchmark Measures: K12 Edtech App Safety

Our primary focus was measuring potential and actual safety risks in K12 Edtech apps. A key part of this research entails calculating an ISL Safety Score for each app.

4.2.1.1 The ISL Safety Score

The ISL Safety Score is a new safety scoring rubric based on the observed and measured behavior of the apps themselves. The ISL Safety Score expands on the predicted risk based on SDKs included in the app by adding in observed app behaviors. There are three key components to the ISL Safety Score:

- Measured Risk: SDKs included in the app and their risk ratings,
- Observed Risk: Observed network traffic to what we refer to as the "big six" data aggregators (Adobe, Apple, Amazon, Facebook, Google, and Twitter), and
- Observed bad behaviors:
    - Advertising presence,
    - Retargeting advertising presence,
    - WebView use,
    - Dangling domain presence,
    - Inclusion of Max Preps (an advertising supported platform analyzed by us in Spotlight Report #4).

Important to note that the scoring criteria for this benchmark are unique to the domain of K12 Edtech. For a different industry vertical (such as FinTech, for example) the scoring categories will be the same, but the criteria/thresholds will be different.

There are four possible outcomes for the ISL app Safety Score:

- **Some Risk:** This represents the "safest" of all safety scores. Note that "no risk" is not an option in our scoring rubric as all apps entail some level of risk.
- **High-Risk:** This represents the middle tier of safety risk. Apps that receive this rating meet at least one of the following criteria:
    - Presence of high-risk SDKs (at least one Very High Risk or High Risk SDK).
    - App's use of Webview.
    - Presence of data aggregators: Google or Apple, as determined from either the presence of SDKs or from network traffic analysis.
    - Presence of one or more dangling domains in the app.
- **Do Not Use:** This score represents the least safe apps and ISL recommends that these apps are not safe for students. Apps receive this score if they meet at least one of the following criteria:
    - Presence of advertising (of any kind). The safety score doesn't distinguish between contextual and retargeted advertising in K-12 ed tech apps, since no matter what kind of advertising is present, student data is being shared/leaked into advertising networks. This is dangerous because there is no way for the public to inspect where the data goes or how it's used.
    - Presence of one or more Data Broker SDKs (per the California and Vermont Data Broker registries).
    - Presence of data aggregators: Facebook, Amazon, Twitter, or Adobe, as determined either by the presence of SDKs or from network traffic analysis.
    - Presence of MaxPreps. Refer to our earlier research which deeply examines the extremely risky behavior of MaxPreps, an advertising school sports platform [owned by CBS/Viacom, parent to Disney] used

by hundreds of schools. https://internetsafetylabs.org/resources/reports/spotlight-report-4-me2b-alliance-product-testing-report-deeper-look-at-k-12-school-utility-apps-uncovers-global-advertising-company-from-cbs-viacom-unexpected-security-risks/
    - App uses resources without asking for and receiving permission.
- **Unable to Test:** We were unable to test several apps due to a variety of reasons:
    - App required school login credentials in order to exercise even basic functionality.
    - App was broken.
    - App was a paid app.

Table 4.1 summarizes the ISL Safety Scoring rubric.

Table 4.1 ISL App Scoring Rubric

SOME RISK	HIGH RISK	DO NOT USE	UNABLE TO TEST
	Presence of at least one (1) SDK that is High Risk or Very High Risk	Presence of advertising (any)	Login required and there's core functionality that we weren't able to access as a result
	WebView Use	Presence of one (1) or more registered Data Broker SDKs	Paid app
	Presence of up to two (2) of the following data aggregator platforms (SDKs or NW traffic): Apple, Google	Presence of one (1) or more of the following data aggregator platforms (SDKs or NW traffic): FB, Amazon, Twitter, Adobe	Broken App
	Presence of a dangling domain	Presence of MaxPreps	

4.2.1.2 Potential Versus Observed Safety Harms

Our original 2021 research measured *potential* and likely safety harms that were derived by analyzing the SDKs present in an app. This current benchmark improves upon that by also including *observed*, actual safety risks measured by assessing the app's network traffic flow. Table 4.2 summarizes the app behaviors measured in the benchmark.

Table 4.2 Measured Risks and Harms

RISKS	OBSERVED HARMS
Volume and risk categories of SDKS in the app.	Network traffic analysis, including noteworthy 3rd parties (aggregators or data brokers) receiving student data.
Types of data collected or accessible by app.	Presence of advertising (of any kind).
App use of WebView.	Presence of dangling domains.

4.3 Scope of the Benchmark

This benchmark evaluates technology in use across all 50 states plus the District of Columbia by examining the behavior of mobile app versions of technologies recommended or required by schools, as identified through examination of school and district websites. NOTE that schools (students, parents) may be using webservice versions of the technologies and not always the app. We did not measure webservice behavior, but we expect it to be comparable. It is possible that webservice behavior will turn out to be worse due to cross-site trackers.[1]

We randomly sampled 13 schools in each state and identified and evaluated all the apps used by the schools. This resulted in the analysis of 663 schools, and identification of 1722 apps (or digital technologies) in use across schools in the sample.

Table 4.3 Sample Summary

Total # of Schools	Total # Apps Recommended or Required by Schools	Total # of Apps Scored
663	1722	1357

Broken and paid apps were not tested in this research. Note that the total number of apps scored is higher than the total number of apps tested due to our ability to

[1] While there are various theoretical mitigations sometimes possible in browsers and not possible in apps, these mitigations are not meaningfully useful by students.

identify "Do Not Use" apps through the presence of advertising/Very High-Risk SDKs. As our research made clear, SDKs risk analysis has proven to be extremely accurate as compared to observed network traffic. Section 5.6 provides the network traffic analysis.

4.4 Types of K12 School Apps (Edtech Typology)

In expanding the research scope from School Utility Apps to *all* Edtech apps, we needed a K12 Edtech typology to categorize and compare apps by type. We discovered early on, however, that there is no single definitive typology that categorizes all the types of K12 Edtech in use. Thus, we evaluated several different categorization schemas to arrive at a final typology, mainly based on G2's Edtech taxonomy (see Appendix A for details).

We added the category, "Non-Education Specific", due to the recommendation of many general purpose technologies/websites/apps by schools. Each app identified in the research was assigned to one of these categories.

4.5 Key Research Questions

Our original research (Spotlight Report #1) unveiled several disturbing findings regarding the safety of school utility apps. Thus, we were interested to understand the following key questions about K12 edtech in use across the US. All of the questions are noted here, though this report only addresses the questions in bold. Answers to the other questions will be provided in the reports described in Section 4.1.

1. **How safe *is* the most commonly used K12 Edtech in the US?**
    a. **What student data is being collected by these apps?**
    b. **What third parties (data processors) have access to student data in the apps?**
    c. **What third parties (data processors) are receiving students' data?** Particularly for kids under the age of 10 (5th grade)?
    d. **How often is student data being shared with corporate entities, and advertising entities in particular?**
    e. **How much in-app advertising are students being exposed to?**
        i. **How much *targeted advertising* are students being exposed to?**
    f. **How often do we see dangling domains apps?**
    g. **How often do we see hijacked/malicious domains in apps?**
    h. **Which apps are presenting the most safety and privacy risks to children?**
    i. What are the greatest safety and privacy risks to children?
    j. **How risky are the most widely used apps?**
2. How many schools in the US are exposing students to risky technology?
3. Are there particular app developers that are riskier than others?

4. Are there differences in the safety of K12 Edtech in use based on geographical region, population density, ethnicity/race, income level, or public/private school, and custom vs. generic?
    a. School grade level
5. **Are there differences in the safety of K12 Edtech in use based on type of app?**
6. Are apps that are "certified" by typical Edtech certifications safer than those that aren't?
7. Are parents/students being informed about the data processing in technology mandated or recommended by schools?
    a. Do they provide written consent or permission, and does it cover all the technology in use?
        i. Are there patterns of behavior based on region, population density, income level, ethnicity/race, or public/private schools?
    b. How much technology is off the shelf and how much is contracted through the school or the district?
8. What kind of technology vetting are schools performing?
    a. Are there patterns of behavior based on region, population density, income level, ethnicity/race, or public/private schools?
9. What effects are regulations having on schools and K-12 edtech?
    a. What kind of effect is COPPA having on the safety of ed tech used in K-12 schools?
    b. What kind of effect is COPPA having on schools' technology choices and vetting behaviors?
    c. What regulation seems to be having the most positive impact on tech safety?
10. What information do 3rd parties get from the website trackers?
    a. How many school websites have risky trackers?
        i. By total, region, school type (public/private), population density, income level, ethnicity/race.
    b. Which companies have the most trackers on school websites?

5 National Findings

5.1 General Summary Data

5.1.1 Schools

As noted earlier, we analyzed 13 schools in every state and the District of Columbia, ensuring an evenly distributed mix of grade level, weighted by geography category (obtained from the National Center for Education Statistics Search for Public Schools (ed.gov)). We also included one (1) private school in each state, resulting in 7.8% of the sample being private schools, closely approximating the 9% of students enrolled in private schools in the US[2], though not resulting in enough data for us to represent private school behavior within a state.

We feel this sampling methodology is a viable reflection of the entire nation and as such, our results can be extrapolated across the US public schools with reasonable confidence. (See Section 8 for more details on our sampling methodology.)

Table 5.1 All Schools in Benchmark Sample by Grade and Public/Private

Elementary School	Middle School	High School	Private School (any grades)
204	204	204	51

Table 5.2 Public Schools in Benchmark Sample by Geography

Rural	Suburban	Town	City
154	195	99	164

Table 5.3 Private Schools in Benchmark Sample by Geography

Rural	Suburban	Town	City
5	18	3	25

Appendix B includes the list of all schools by state included in this benchmark.

[2] https://nces.ed.gov/fastfacts/display.asp?id=55 Accessed on 11/26/22.

5.1.2 Apps

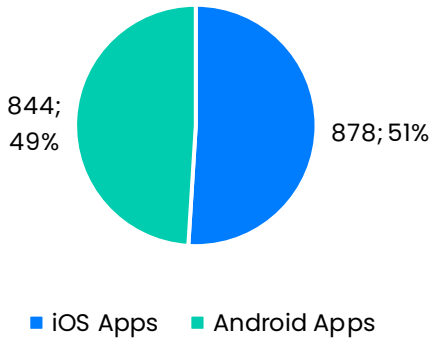
As noted earlier, from the analysis of the 663 schools, 1722 apps were identified as either recommended or required by the school or the district[3]. Of those 1722 we were able to score 1357. The charts in this section describe the sample set by operating system (iOS vs. Android), Custom vs. Generic, and by Edtech category.

5.1.3 App Sample Key Findings

- Most apps were Community Engagement Platform (CEP) apps, Non-Education Specific (NES) apps, and Other (O) apps. The apps tested in these three categories made up 77% of all tested apps.
- 85% of NES apps were not designed for exclusive use by children.
- 81% of O apps *were* designed for use by children.
- In total, at least 481 (28%) of the apps in the sample were not designed for exclusive use by children.
- There were slightly more iOS apps (51%) than Android apps (49%) in the total list of apps. Similarly, of the 1357 apps tested, 51% were iOS and 49% were Android.

5.1.4 All Apps

Figure 5.1 — All Apps by OS



[3] We looked at the district websites in addition to the school websites, since the district commonly chose (and licensed) technology for use by all schools in the district.

Figure 5.2 — All Apps by App Category

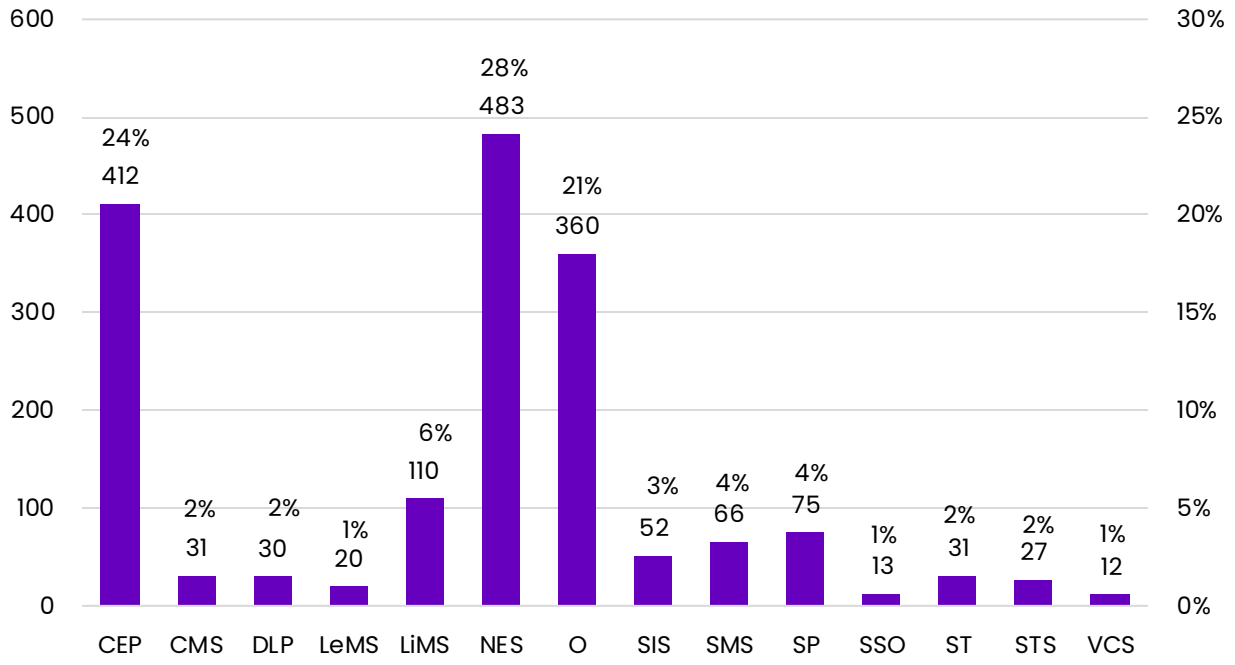
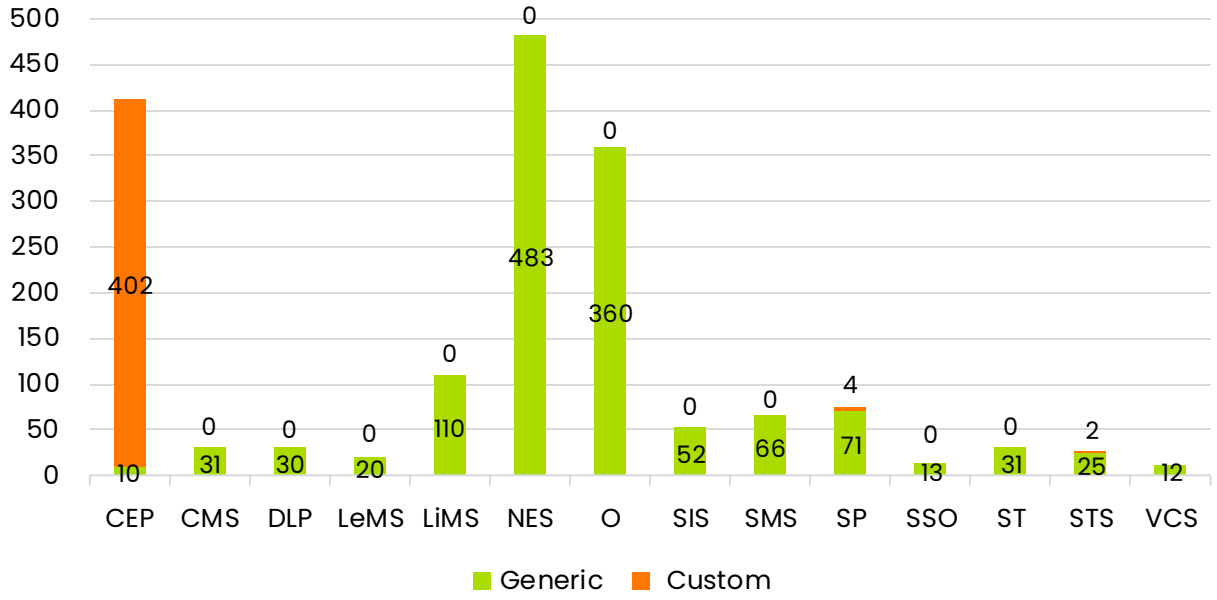


Figure 5.3 — All Apps by Category and Custom vs. Generic



5.1.4.1 NES and O Apps for Adults vs. Children

Since the Non-Education Specific (NES) and [edtech] Other (O) comprised nearly 50% of the technologies being either recommended or required by schools, we further categorized those apps to indicate if they were clearly targeted and built for kids or not. Not surprisingly, most (85%) of the NES apps were *not* designed for

children, but 81% of the O apps were. When combined, 57% of the apps in the NES and O categories were *not* designed for children.

According to this analysis, at least 476 (28%) apps in the sample weren't for children.

Note that we didn't perform this analysis on apps in the remaining categories so it's sure to be low. (For instance, the VCS category includes tools like Zoom and Microsoft Teams, which are not designed for kids.)

Figure 5.4 — NES Apps for Children

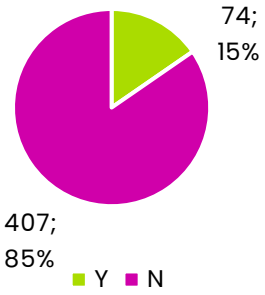


Figure 5.5 — O Apps for Children

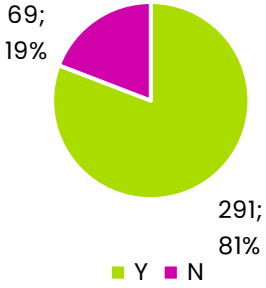
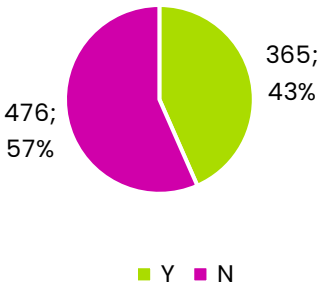


Figure 5.6 — NES & O Combined for Children



5.1.5 Scored Apps

Of the 1722 apps in our sample, we were only able to score 1357 apps. There were three contributing factors for being unable to score an app:

1. The app was broken,
2. The app required a school login, or
3. The app was a paid app.

In total there were 365 apps in the list that were not scored due to the above three reasons. This section provides characteristics of the 1357 scored apps.

Figure 5.7 — Scored Apps by OS

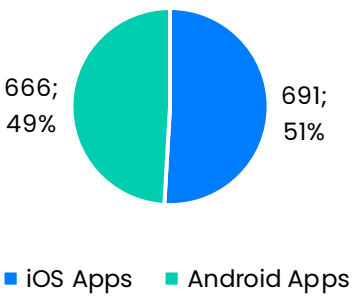


Figure 5.8 — Scored Apps by Category

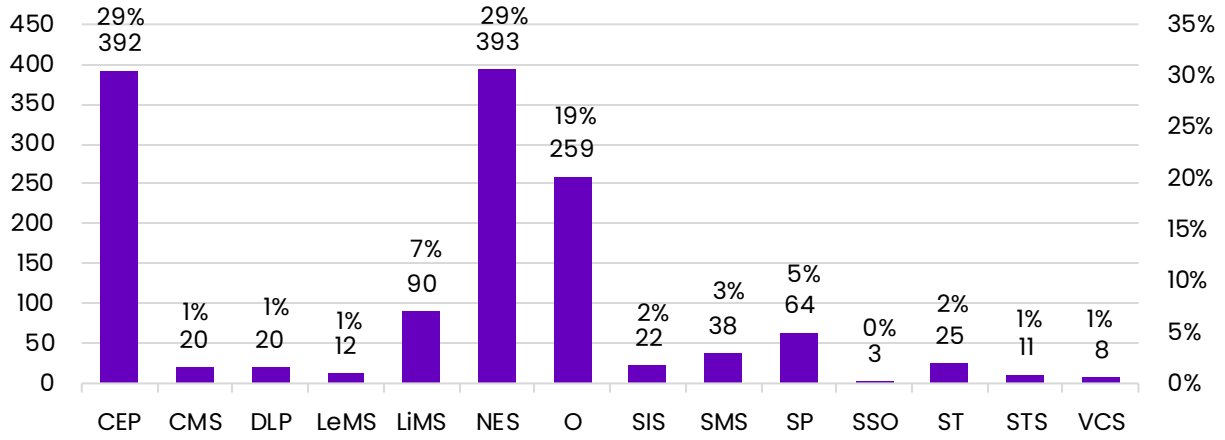
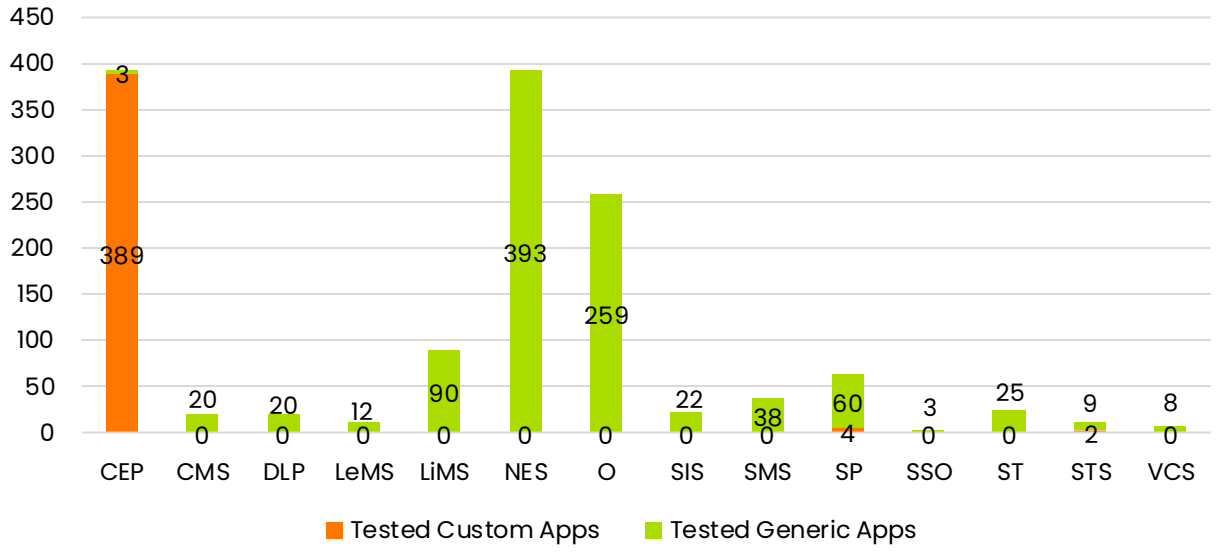


Figure 5.9 — Scored Apps by Category and Custom Vs. Generic

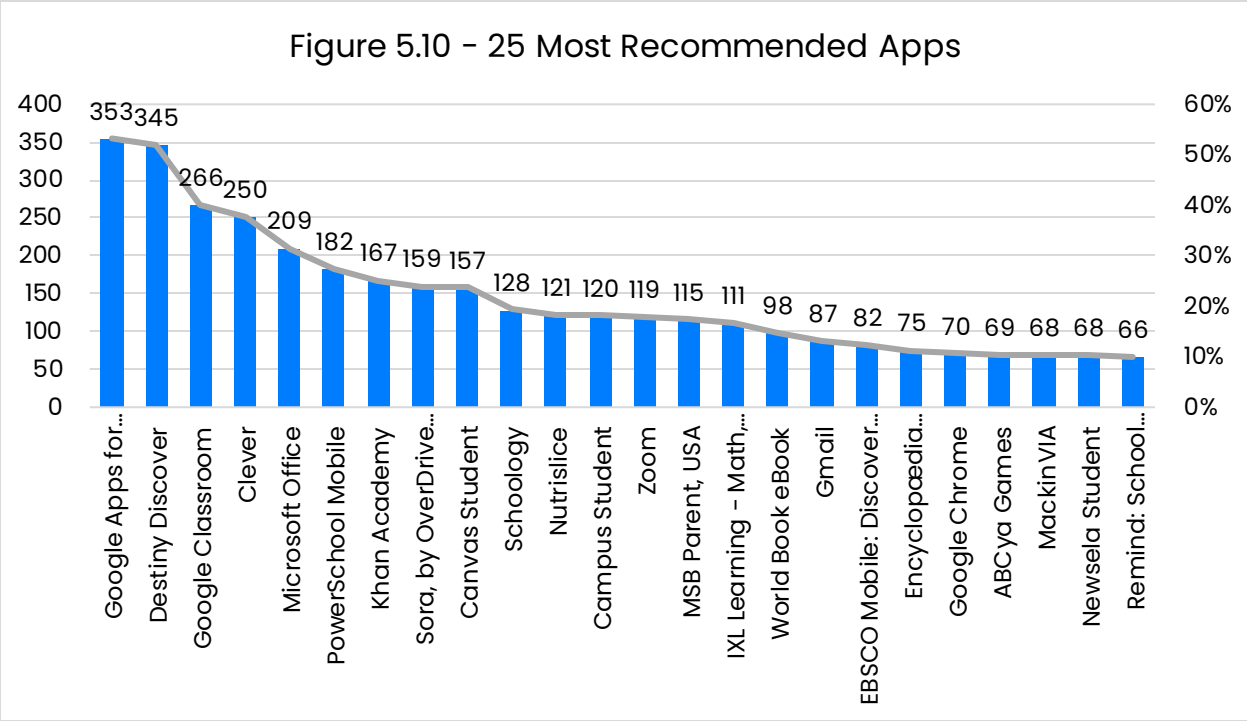


5.1.6 Most Recommended Apps

5.1.6.1 Most Recommended Apps Key Findings

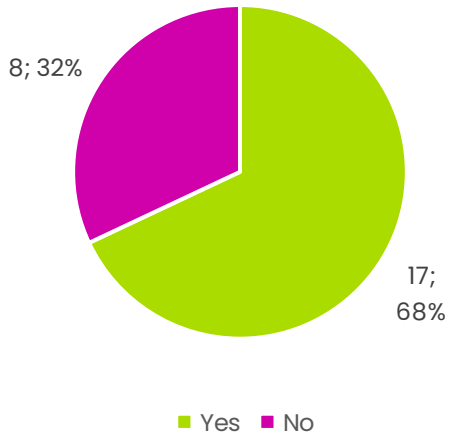
- There is substantial **overlap** between the most frequently **recommended** technologies and the most frequently **required** technologies: **68%** of the top 25 most recommended apps also appear in the top 25 most required apps.
- The most recommended apps represent a broad distribution of app types, with the highest categories being NES, O and LiMS.
    - Because most CEP apps are custom apps named for the school, they don't appear in the most recommended apps, but they are among the most recommended at 39% of the schools providing custom apps.

5.1.6.2 25 Most Recommended Apps



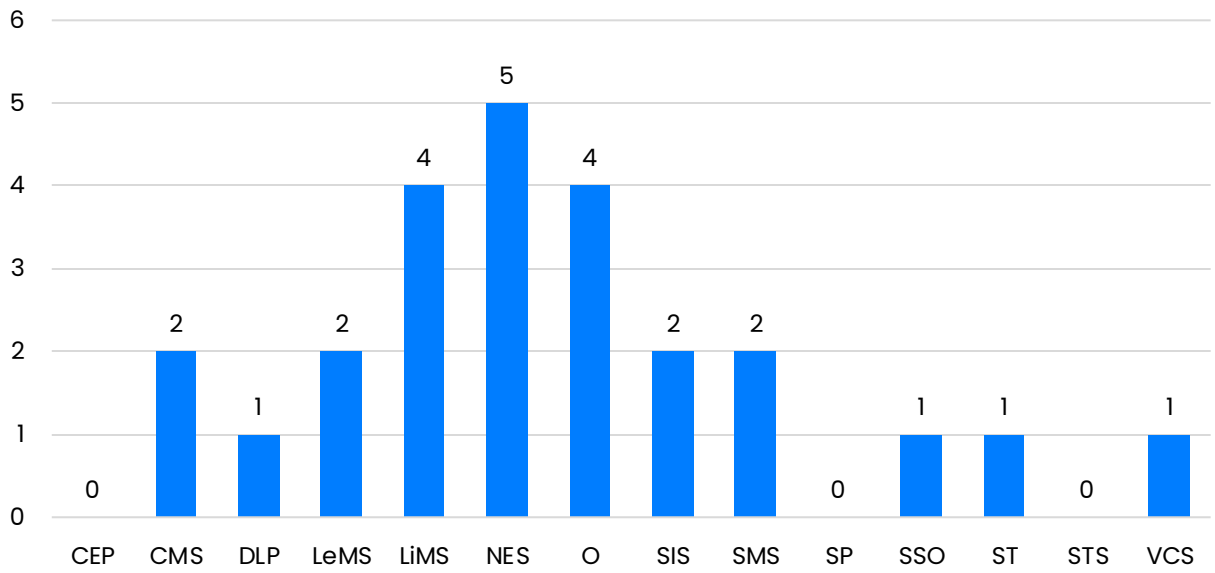
5.1.6.3 Overlap Between Most Recommended and Most Mandatory Apps

Figure 5.11 — % of Most Recommended Apps Also Most Required



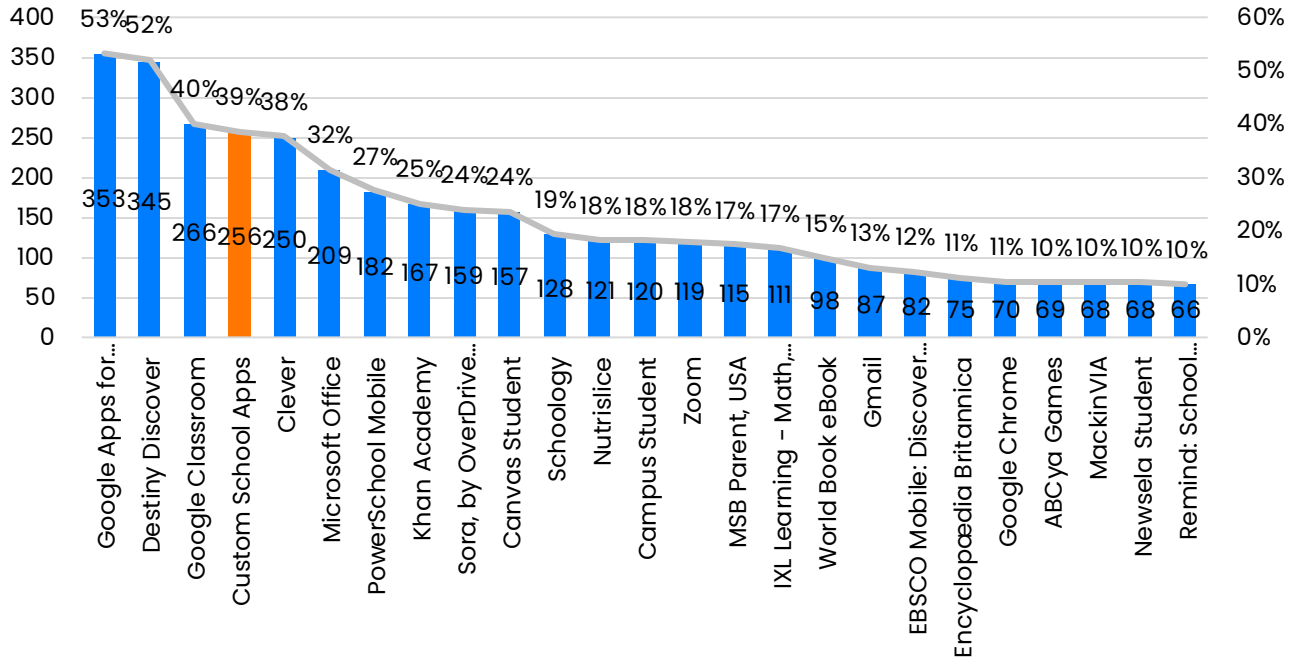
5.1.6.4 Most Recommended Apps by Category

Figure 5.12 — 25 Most Recommended Apps by Category



The above Figure 5.12 points out a critical problem with looking at unique instances of apps in the data set. It looks like no CEP apps are recommended, but in fact, custom school apps (i.e. CEP apps) were among the most frequently recommended by schools. Since the apps all have unique names, they didn't make it into the most frequently recommended list. Figure 5.13 depicts the most frequently recommended list if we regard all CEP apps as a single app (Custom School Apps, with 256 occurrences, i.e. 39% of the schools had custom apps for students).

Figure 5.13 — Most Recommended Apps - With Custom Apps



5.1.7 Most Frequently Required Apps

We designated certain apps as Mandatory or Key for a school if it met certain criteria (described in Section 7.2.1). Note that the schools do not typically specify a particular operating system (OS), so a mandatory app usually reflects both the iOS and the Android versions of the app. Note also that these are unconfirmed with the schools, so the data around the mandatory/key apps is directional in nature and not conclusive.

5.1.7.1 Key Mandatory App Findings

- PowerSchool Mobile, a Classroom Messaging Service type of technology, was the most frequently required at 28% of the sampled schools.
- Google Classroom, a Learning Management System, was second with 27% of all schools requiring it.
- Clever, a Single Sign On service, was third with 24% of schools requiring it.
- The top 25 mandatory/key apps represented a diverse range of edtech categories, no single category dominated, though School Management Software (SMS) was the highest with 4 apps in the top 25.
- Google developed the most apps in the top 25 required apps with five (5) apps.
- Microsoft was the only other developer with more than one app in the top 25 mandatory apps with two (2) apps.

- It's not surprising that Google and Microsoft apps were the most frequently mandatory, since many schools provide Gmail or Outlook accounts to students, as well as requiring the use of Google or Microsoft the productivity apps.

Figure 5.14 — Top 25 Mandatory/Key Apps

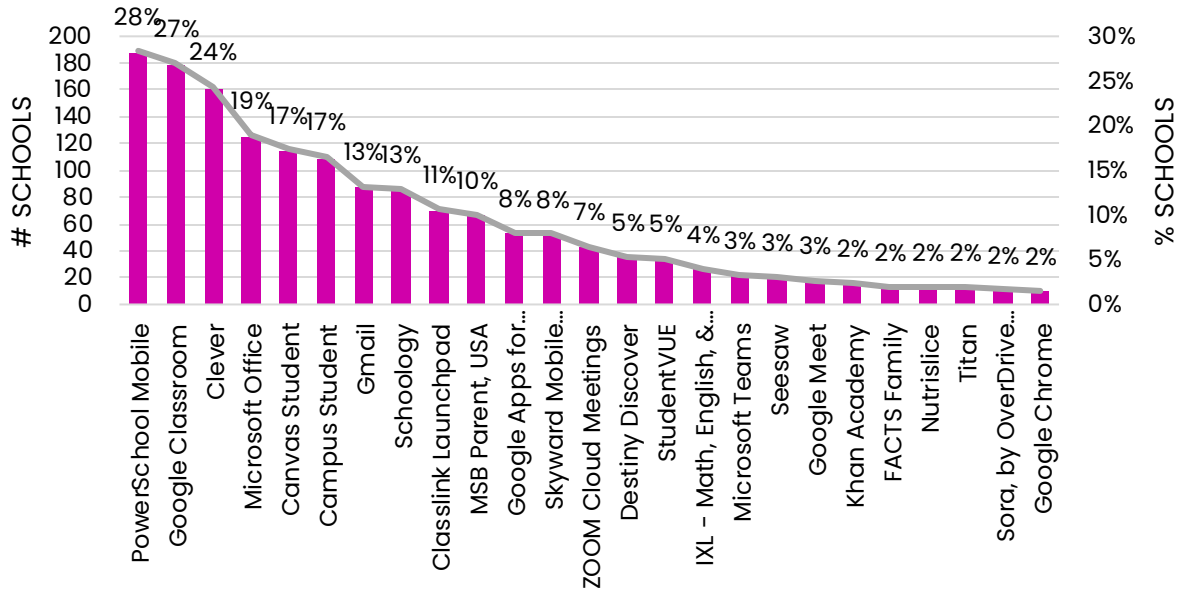
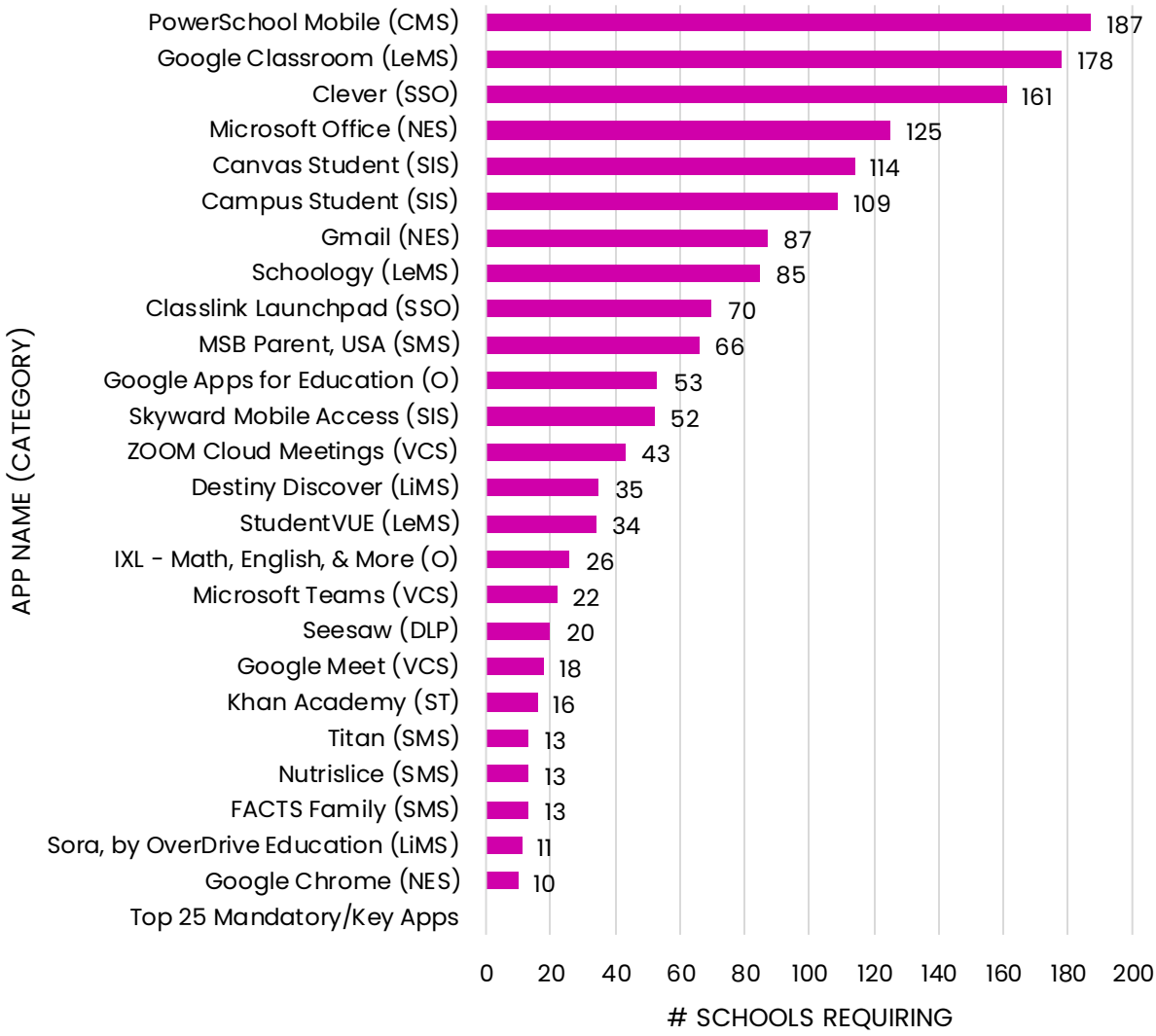
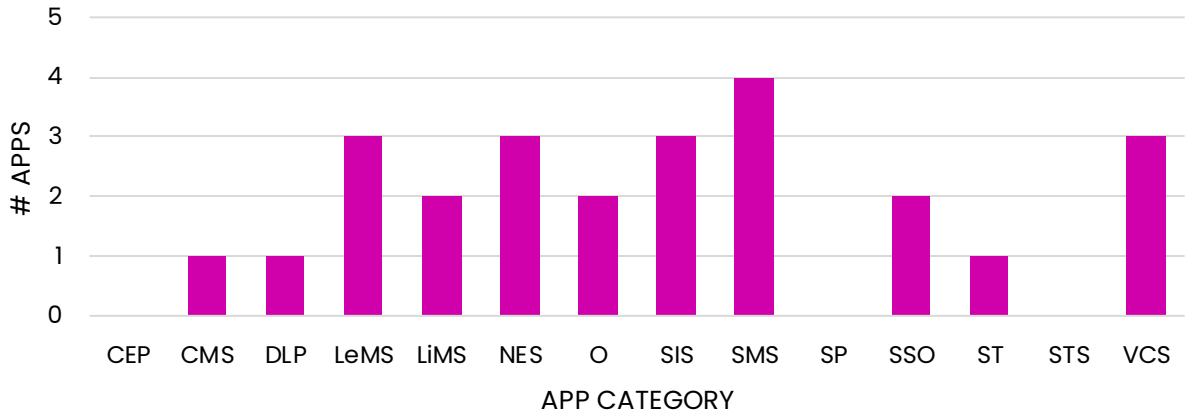


Figure 5.15 — Top 25 Mandatory/Key Apps



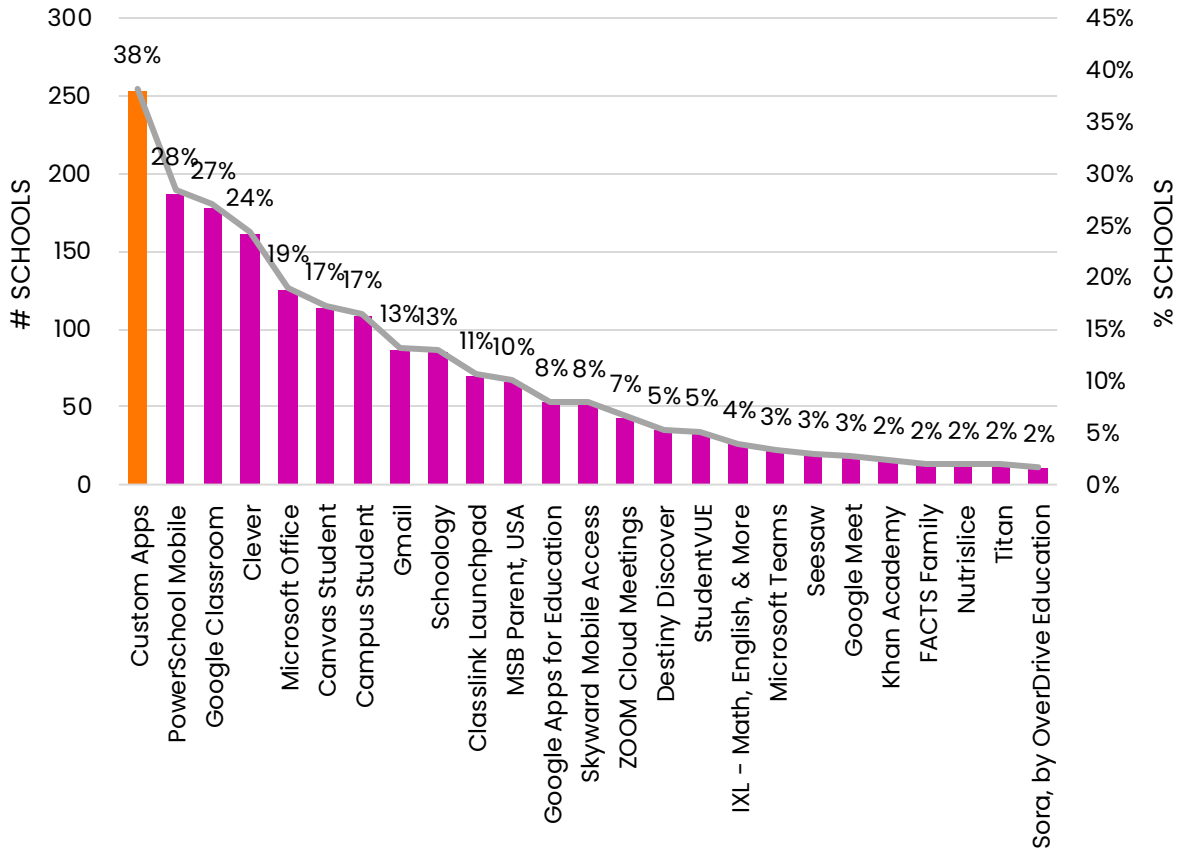
In general, there was a wide variety of edtech categories represented by the top 25 required apps (see table xxx below).

Figure 5.16 — Top 25 Mandatory/Key Apps by Category



Similar to Section 5.1.6.4 above, if we regard all the custom apps as a single app, they become the most frequently named mandatory or key app (see Figure 5.17).

Figure 5.17 — Top 25 Most Mandatory Apps - With Custom Apps



5.1.8 Number of Technologies Recommended by Schools to Students

In this research, we identified technologies recommended by schools through manual searching of the school and district websites. Occasionally, we would find lengthy lists of technologies recommended, and in some cases vetted and approved by the school or district. Some of these lists were quite long and we chose not to include all the apps contained in big lists in our sample. We did however keep track of the number of technologies contained in these lists.

5.1.8.1 School or District Technology Lists Key Findings

- For schools/districts that had aggregated lists of recommended technologies, the average number of technologies was a staggering 125 technologies.
- For schools/districts that provided lists of approved technologies, the average number of technologies listed was an even more jaw-dropping 172 technologies.
- We found one school with a list of approved technologies topping out at 1411 app (Mountain Phoenix Community School in Colorado).

Table 5.4 School/District Technology Lists

Type of List	# Schools	Average # Technologies	Max # of Technologies
Manual App Count	663	11	61
Simple Aggregated List	266	125	1411
Vetted/Approved Technology List	161	172	1411

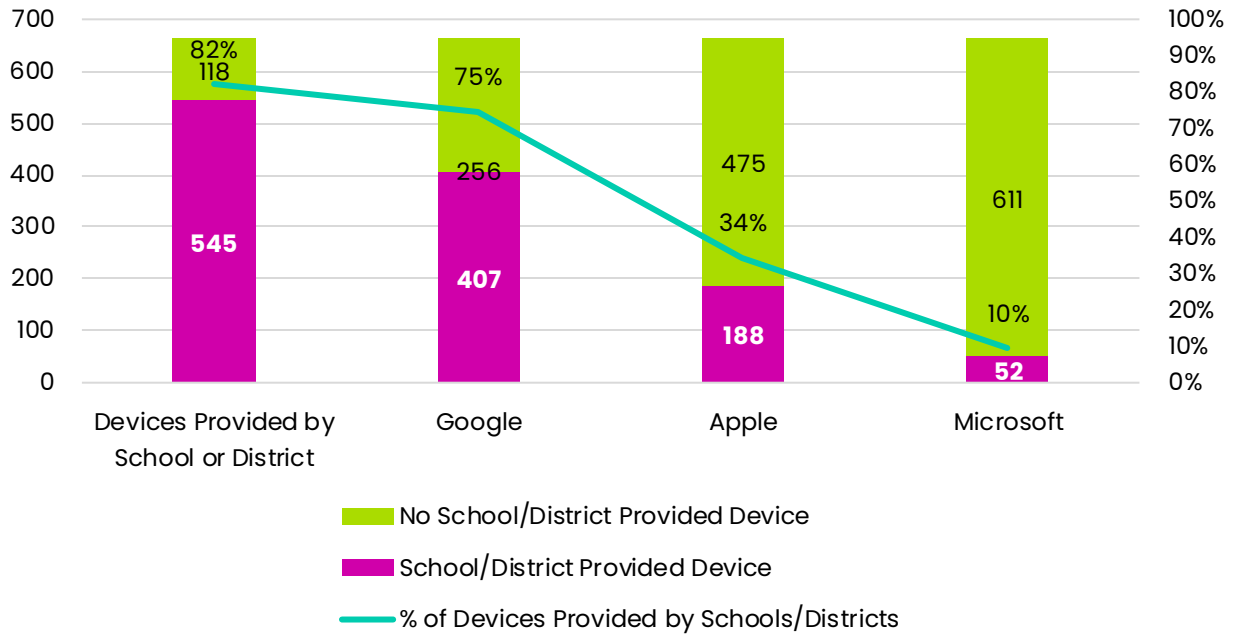
5.1.9 Devices

As part of this research, we identified if schools or districts were providing personal computing devices to students, and what type of devices were being provided.

5.1.9.1 Key Device Findings

- **82% of schools provided computing devices to students.**
- Of schools that provided devices **75% of them provided Chrome OS based devices** (shown as "Google" in Figure 5.18 below), **which was more than double the next closest devices, which were Apple based OS devices**, mostly iPads, especially to grades K-2.
    - We saw many schools issue iPads to grades K-2 and Chromebooks to grades 3-12.

Figure 5.18 — School/District Provided Computing Devices by OS Vendor

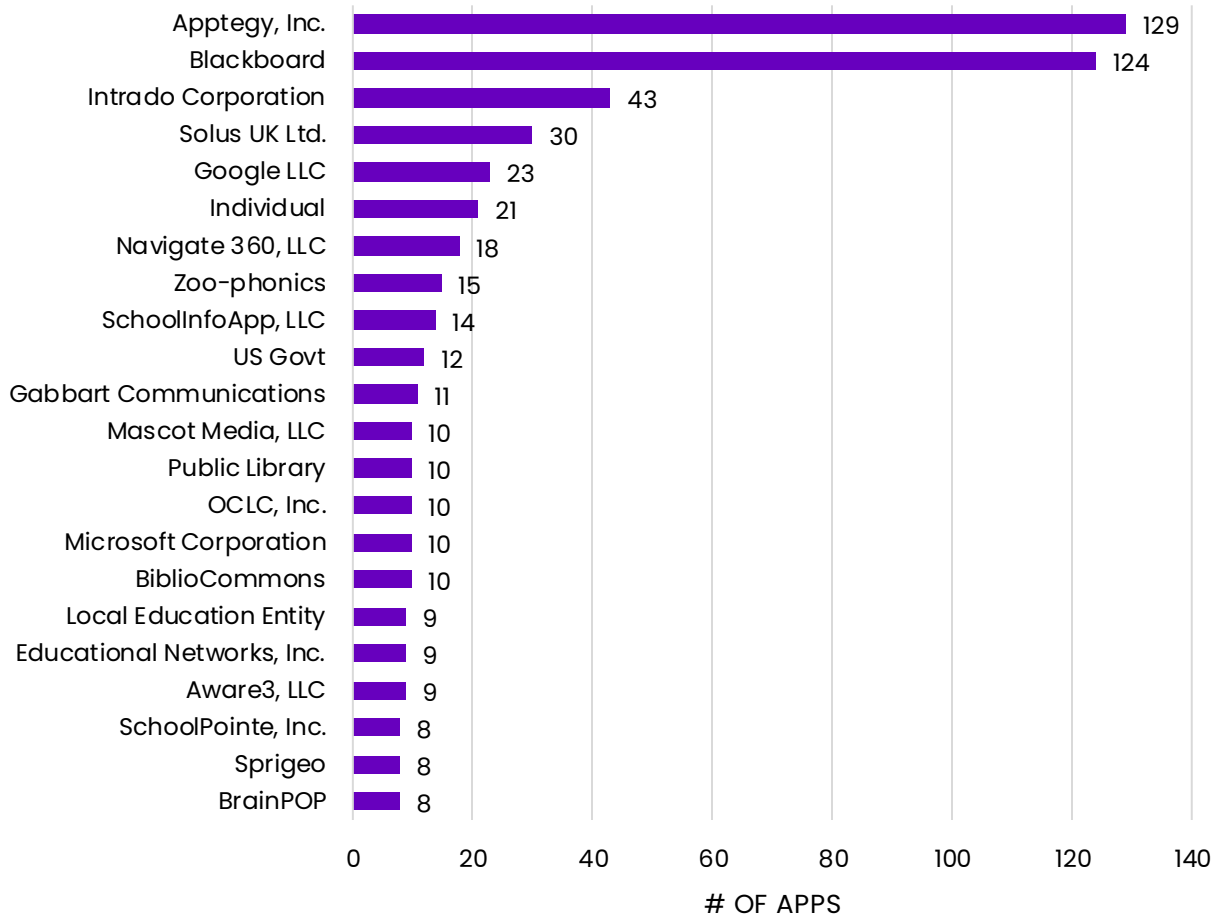


5.1.10 Developers

5.1.10.1 Developer Key Findings

- **The most common developers in the sample set were CEP type app developers, who occupied the top 3 places: Apptegy (129 apps), Blackboard (124 apps), and Intrado (43 apps).**
    - These were also the top three developers in the Custom apps.
- **In the Generic apps, the top three developers were: Solus (LiMS, 30 apps), Google (23 apps) and Navigate 360(SP, 18 apps).**
- The frequency of developer in our sample set doesn't always indicate the most widely used apps. Take for instance Zoo-phonics (15 apps in our sample), which aren't nearly as popular as Google apps with respect to downloads.
- When we look at the most downloaded apps and developers in our sample, it's no surprise that Google, Microsoft and Amazon hold the top three positions.
- Google was the most popular developer of apps in both the most recommended and most required app lists, with 4 and 5 apps, respectively.

Figure 5.19 — Top 22 Most Common Developers



We analyzed the apps also by approximate number of downloads (derived from the information in the Google Play store). Figure 5.20 shows the developers with the most downloaded apps in our sample. The results are unsurprising, mainly due to the fact that some of the world's most popular apps—which are not educational specific (such as YouTube)—are being recommended or required by schools.

Also important to note the vast difference in the volume of downloads between the most downloaded app (Gmail) and the first real edtech app in the top 28 most downloaded apps, Photomath (which received a safety score of Do Not Use, due to several risk factors, including the use of WebView and sending data to Facebook).

Figure 5.20 — Developers of Top 28 Most Downloaded Apps

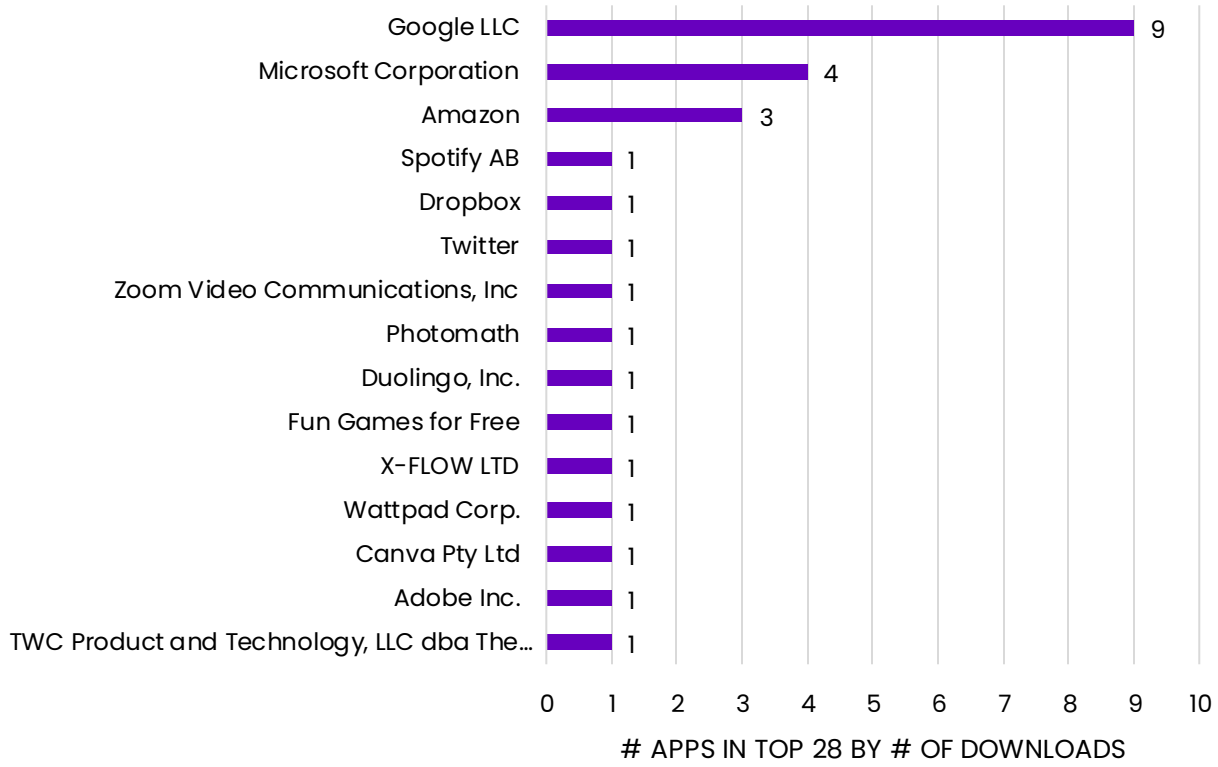
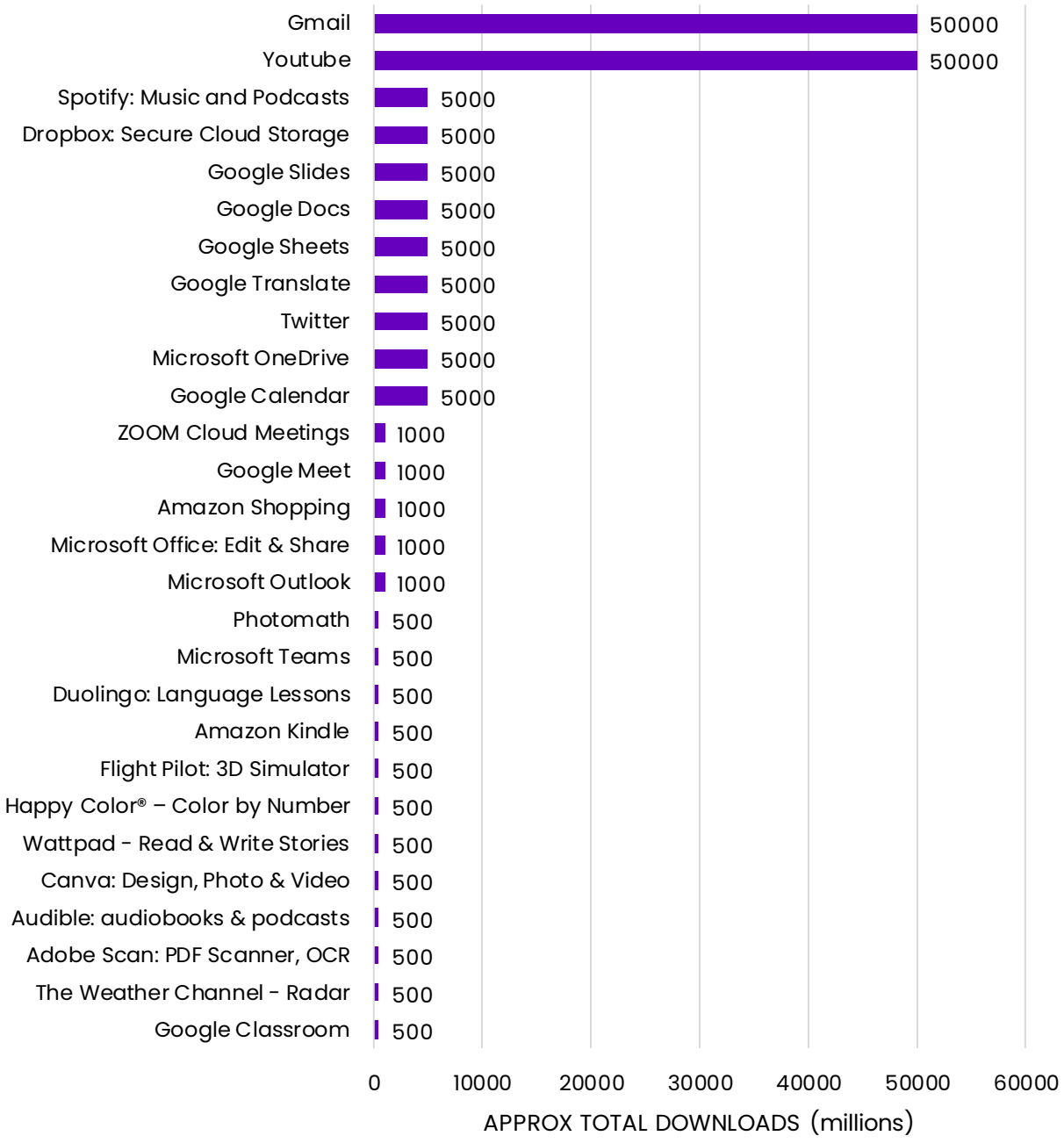
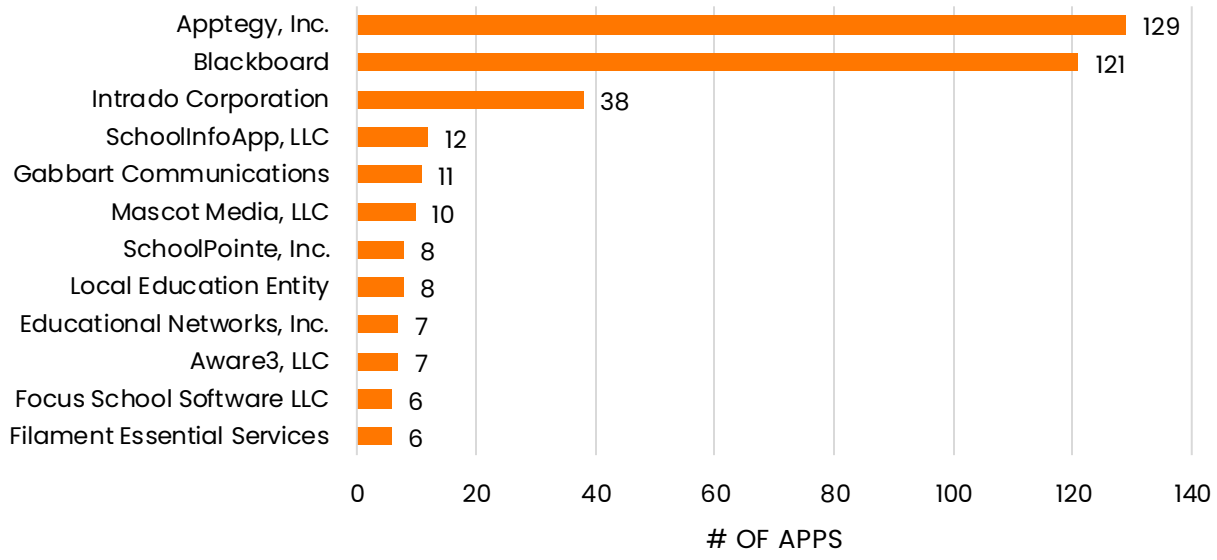


Figure 5.21 — Top 28 Most Downloaded Apps



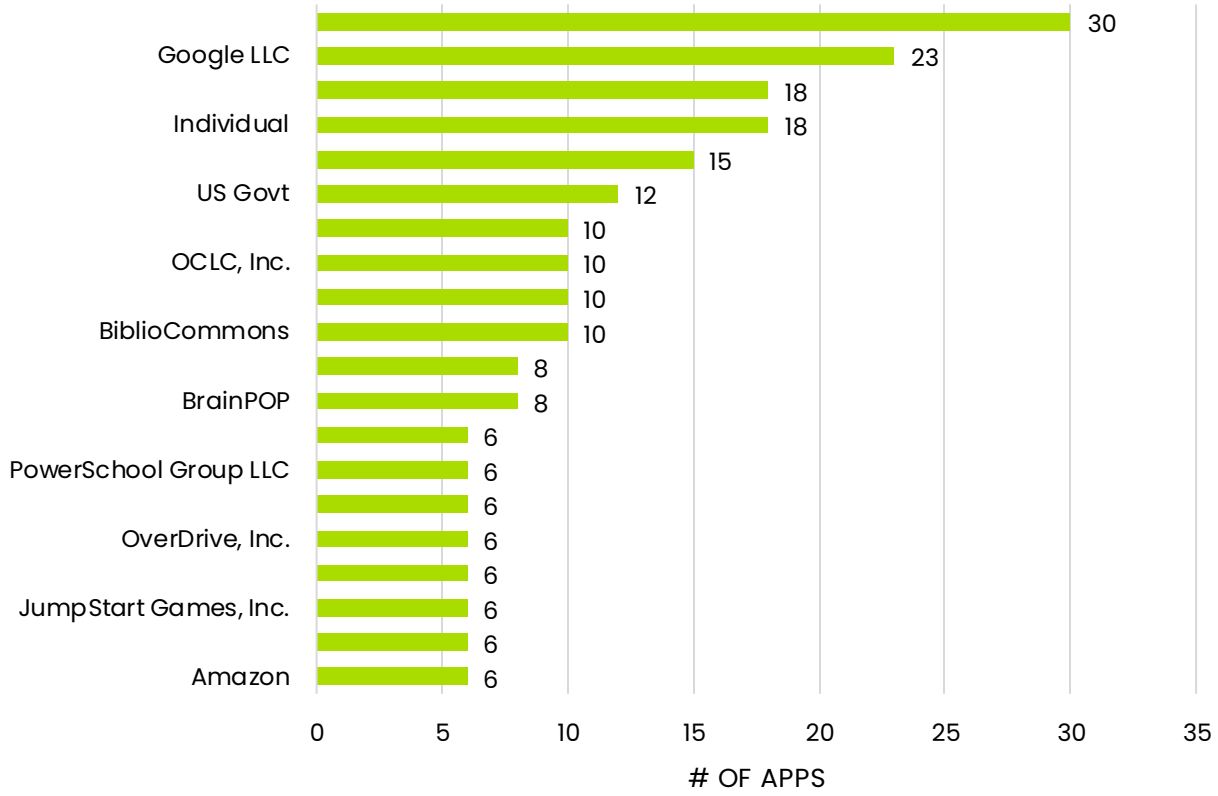
5.1.11 Custom App Developers

Figure 5.22 — Most Common Developers Custom Apps



5.1.12 Generic App Developers

Figure 5.23 — Top 20 Most Common Developers
Generic Apps

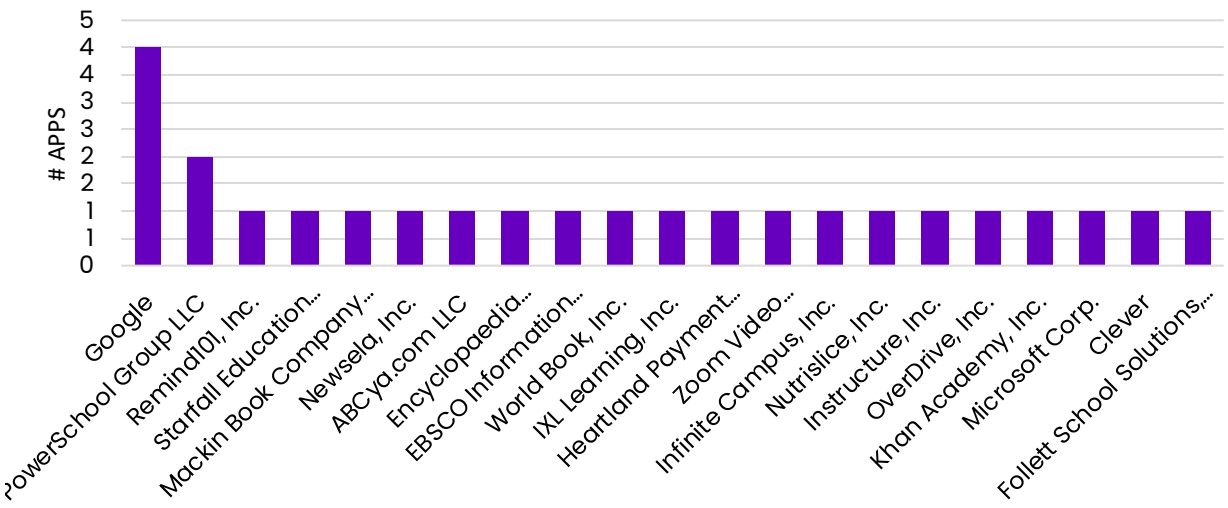


5.1.13 Developers By Edtech Category – See Appendix C

Appendix C contains lists of developers in the sample for each of the fourteen edtech categories.

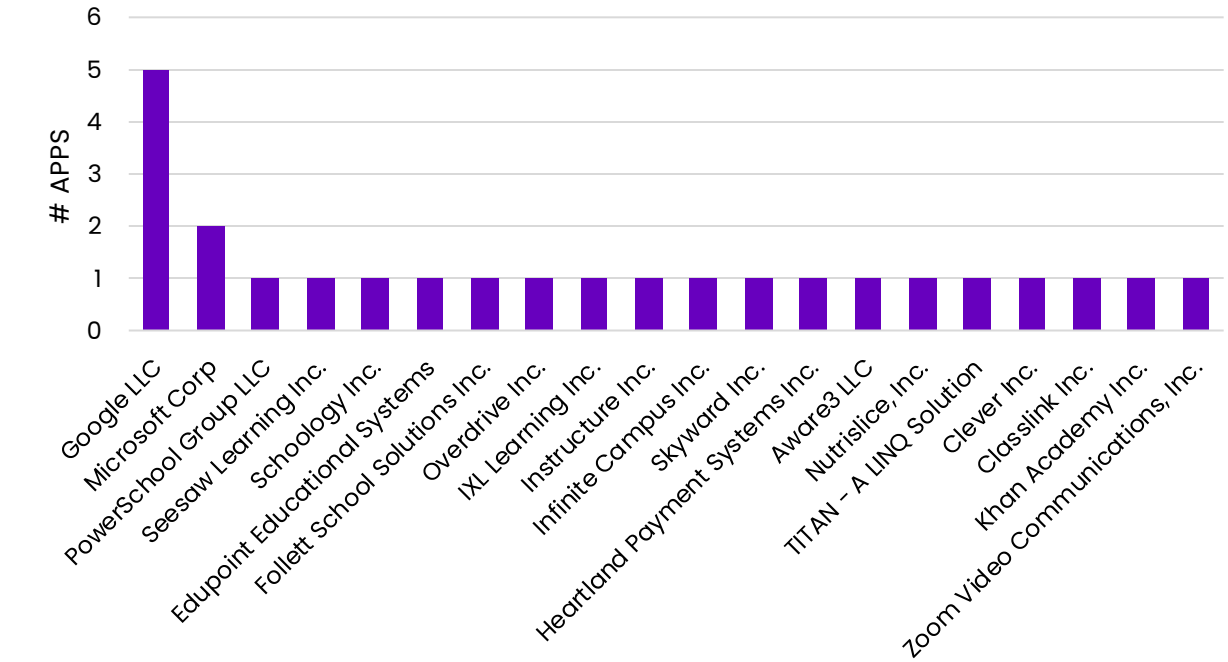
5.1.14 Most Recommended App Developers

Figure 5.24 — Top 25 Recommended Apps by Developer



5.1.15 Most Mandatory/Key App Developers

Figure 5.25 — Top 25 Mandatory/Key Apps by Developer



5.2 App Safety Score Analysis

This section examines the ISL Safety Scores assessed for all the scored apps in the sample (1357 apps).

5.2.1 App Safety Score Key Findings

- **78%** of all tested apps rated **Do Not Use,** and **18%** rated **High Risk.**

- Only **4%** rated our safest score, **Some Risk**.
- **No (0) Custom** apps were rated our safest score, **Some Risk** and **89%** of **Custom** apps were rated **Do Not Use.**
- **Android** apps were somewhat **safer** than **iOS** apps, but both had tiny fractions of apps that were relatively safe for students at 5% and 3% respectively.
    - **80**% of **iOS** apps were rated **Do Not Use** compared to **76%** of **Android** apps.
- **Most recommended apps**: of the apps tested, **86%** rated **Do Not Use**, **9%** were **High Risk**, and only one app **(5%) Some Risk**.
- **Most frequently mandatory/key apps: None** of the apps in the most frequently required apps scored our safest score, **Some Risk**. **74%** rated **Do Not Use** and **26%** rated **High Risk**.

5.2.2 Safety Scores – All Tested Apps

Figure 5.26 — Apps by App Score - All

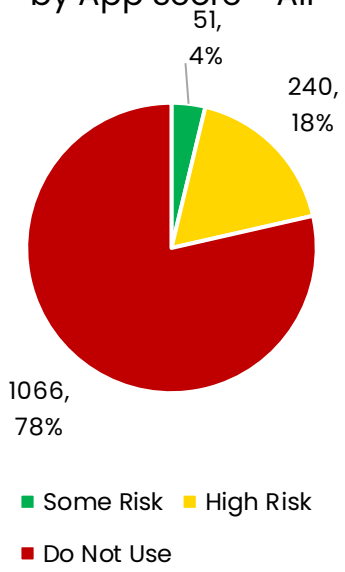


Figure 5.27 — Apps by App Score - Custom

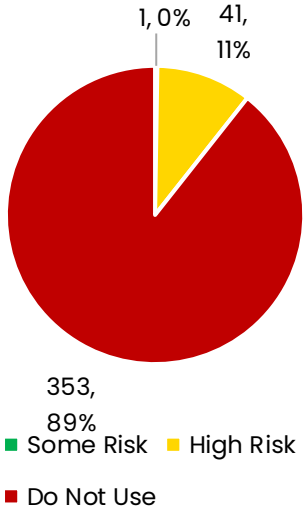


Figure 5.28 — Apps by App Score - Generic

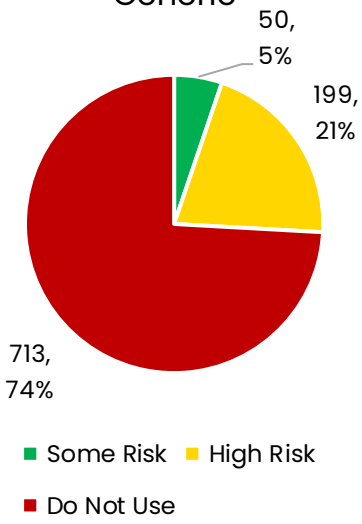
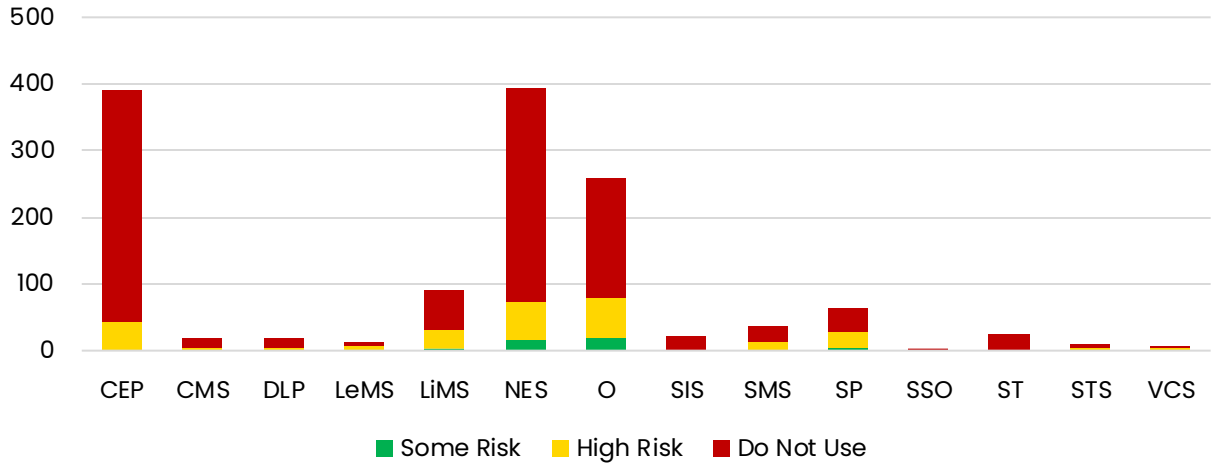


Figure 5.29 — App Scores by App Type



5.2.3 App Safety Scores by OS

Figure 5.30 — Apps by App Score - iOS

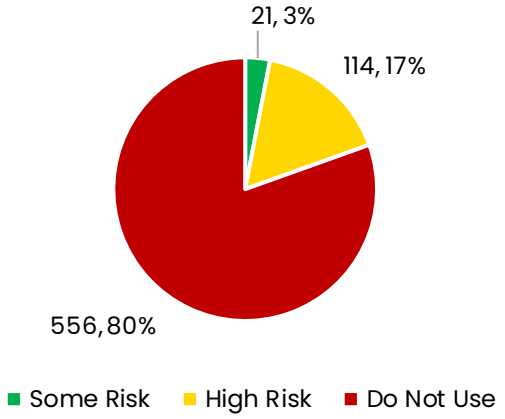
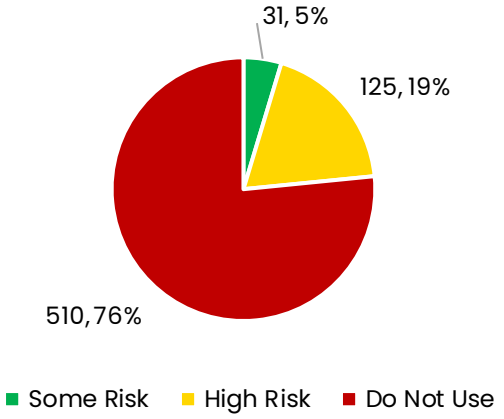


Figure 5.31 — Apps by App Score - Android



5.2.4 App Scores by Most Recommended and Most Required

Figure 5.32 — 25 Most Recommended Apps

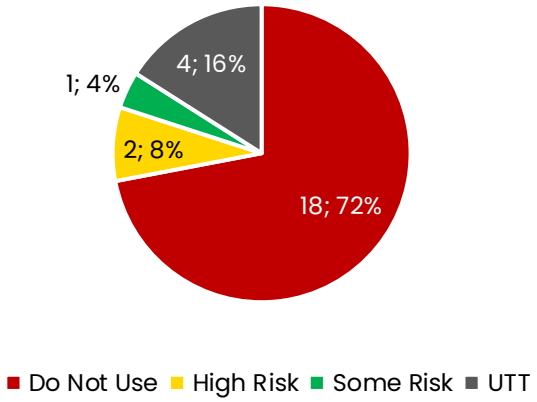


Figure 5.33 — 25 Most Recommended Apps - Tested

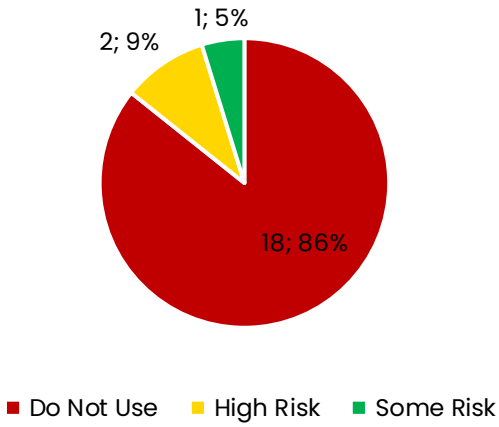


Figure 5.34 — Top 25 Mandatory/Key Apps

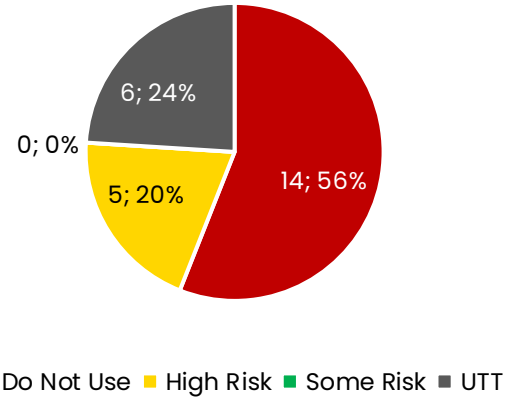
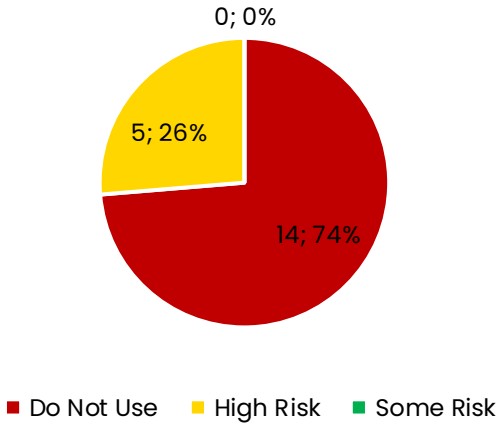
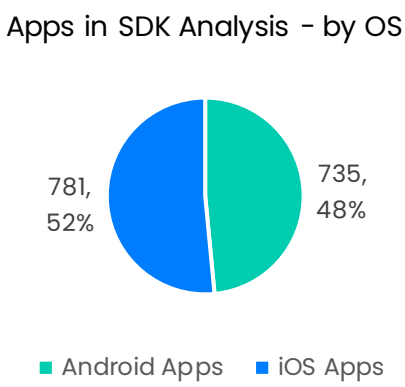


Figure 5.35 — Top 25 Mandatory/Key Apps - Tested



5.3 SDK Analysis

Of the 1722 list of apps, we were able to obtain SDK information for 1516 of the apps. This section examines the SDKs in use by those 1516 apps. Of the 1516 apps analyzed, 52% were iOS and 48% were Android.



5.3.1 SDK Key Findings

- SDKs found in sample:
  - **28%** of the SDKs used in the apps were **Medium or Neutral risk**.
  - **72%** of the SDKs used in the apps were **High or Very High-Risk**.
  - **57%** of the SDKs used in the apps were Very High-Risk, meaning they were advertising or monetization related SDKs.
  - The **Google** Firebase analytics SDK was the most frequently used SDK by apps, appearing **in 67% of all apps with SDKs**.
  - The top 5 SDKs used by apps were **Google** SDKs.
- **94%** of apps have at least **one SDK**.
- Apps with SDKs averaged **9.3 SDKs** per app. That's potentially ten external entities per app.
  - Apps with SDKs averaged **4.4 Very High Risk** SDKs per app.
  - Apps with SDKs averaged **1.6 High Risk** SDK per app.
  - Apps with SDKs averaged **2.1 Medium Risk** SDK per app.
- **76.5%** of all apps included **Very High Risk** SDKs**.**
  - **81.6%** of apps with one or more SDK included **Very High Risk** SDKs.
- **81.3%** of all apps included **High Risk** SDKs.
  - **86.7%** of apps with one or more SDK included **High Risk** SDKs.
- **66%** of apps included one or more **Google SDK**, compared to **36%** of the apps including one or more **Apple** SDK.
  - Note that this is partially due to the fact that while iOS apps can and do include Google SDKs, Google apps do *not* include Apple SDKs.
    - **52.7%** of **iOS apps** included **Google** SDKs.
    - **82.6%** of **Android apps** included **Google** SDKs**.**
- Custom vs. Generic apps:
  - Custom apps were more risky than generic apps. We'd like to see a much bigger difference between the behavior of custom school apps and the generic apps.

        - **Custom** apps average **9.9 SDKs** compared to **9.0 SDKs** for **Generic** apps.
            - **Custom** apps averaged 5.3 **Very High Risk** SDKs per app compared to **4.1** for **Generic** apps.
        - **86.6%** of Custom apps with SDKs had **Very High Risk** SDKs compared to **79.8%** of **Generic** apps.
        - **98.6%** of **Custom** apps with SDKs had **High Risk** SDKs compared to **82.8%** of **Generic** apps.
- iOS vs. Android:
    - Similar to Spotlight Report #1 findings**, Android apps consistently have more and higher risk SDKs than iOS apps**.
        - **Android** apps average **10.8** SDKs compared to iOS apps' 7.8
        - **Android** apps average **6.5 Very High Risk** SDKs, nearly three times as many as **iOS** apps' **2.4**.
    - **89.9%** of **Android** apps included **Very High Risk** SDKs as compared to **63.6%** of **iOS** apps**.**
    - **84.1%** of Android apps include **High** Risk SDKs, compared to iOS apps' **78.6%.**
    - **iOS** apps include more **Medium Risk** SDKs (80.0%) than **Android** with **72.1%.**
    - **70%** of all apps included Google SDKs, compared to **38%** of apps including Apple SDKs.
        - **56.9%** of **iOS apps** included **Google SDKs**, but **Android apps** never included **Apple SDKs**.
    - **iOS** apps were more likely to have zero (0) SDKs than Android apps with **68%** of the apps with no SDKs.
- Most recommended apps:
    - The average number of SDKs found in the most recommended apps was **somewhat higher** at **9.2** per app than for the overall data set at **8.7** SDKs per app.
    - The average numbers of SDKs by risk category in the most recommended apps were slightly better (lower) than for the overall data set.
- Most frequently mandatory apps:
    - The average number of SDKs found in the most frequently mandatory apps were **somewhat higher** at **9.3 per app** than for the overall data set, at **8.7.**
    - However, the average number of **Very High Risk** SDKs was lower at **3.0** than the overall data set at **4.1**.

5.3.2 SDKs Found in Apps by Risk Score

This section shows the breakdown of the SDK Risk Scores for the SDKs found in the apps, and also within the Custom and Generic apps.

Figure 5.36 — SDK Count Across All Apps

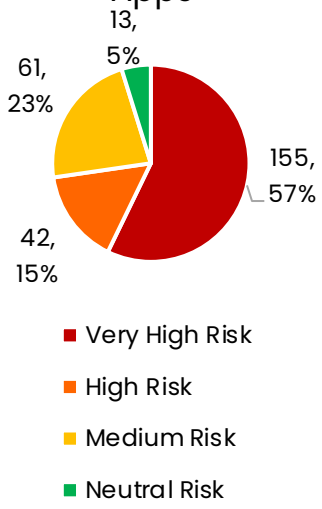


Figure 5.37 — SDK Count - Custom Apps

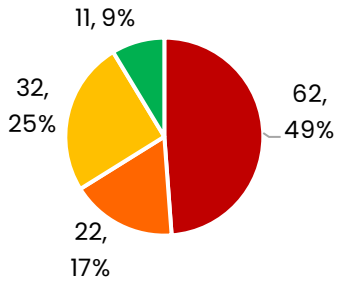
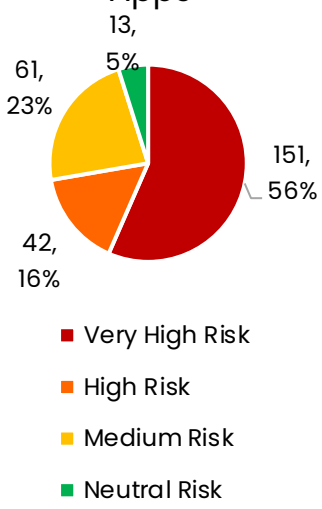


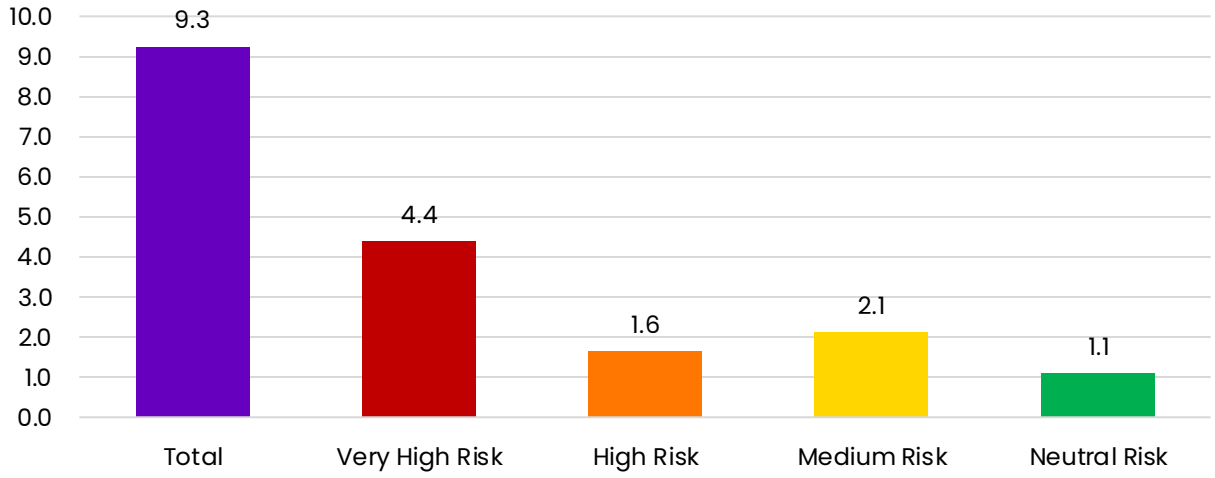
Figure 5.38 — SDK Count - Generic Apps



5.3.3 Average Number of SDKs per App

Apps with at least one SDK averaged 9.3 SDKs. This is somewhat lower than the average of 10.6 SDKs reported in Spotlight Report #1 but is expected since the apps in Spotlight Report #1 were all Custom/CES apps, which had an average of 9.9 SDKs per app in this benchmark (see Figure 5.41).

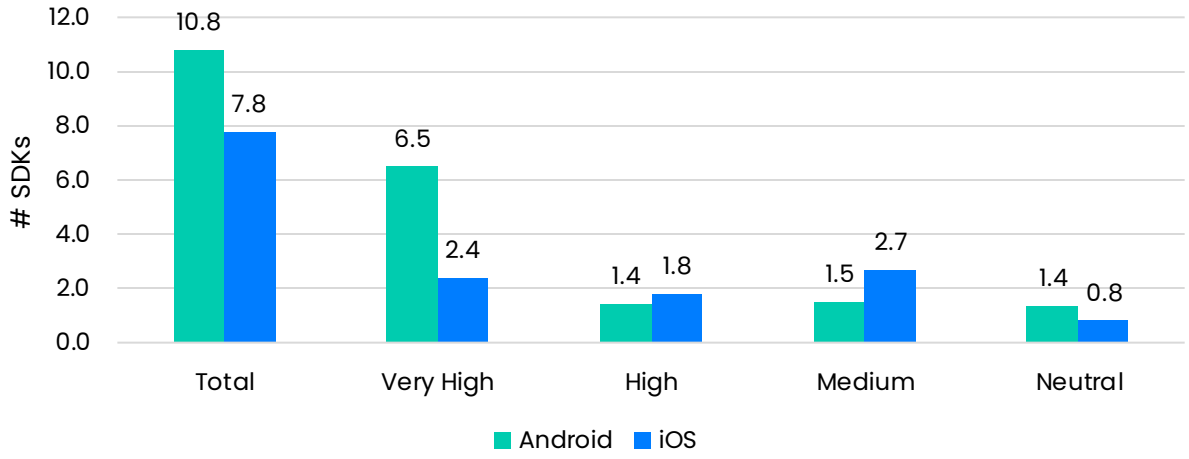
Figure 5.39 — Average # of SDKs in All Apps



5.3.3.1 Average Number of SDKs per App by OS

Similar to Spotlight Report #1 findings, Android apps have more SDKs in general than iOS apps, and 2.7 times as many Very High Risk SDKs than iOS apps on average. iOS apps, however, have somewhat more High and Medium Risk SDKs than Android apps.

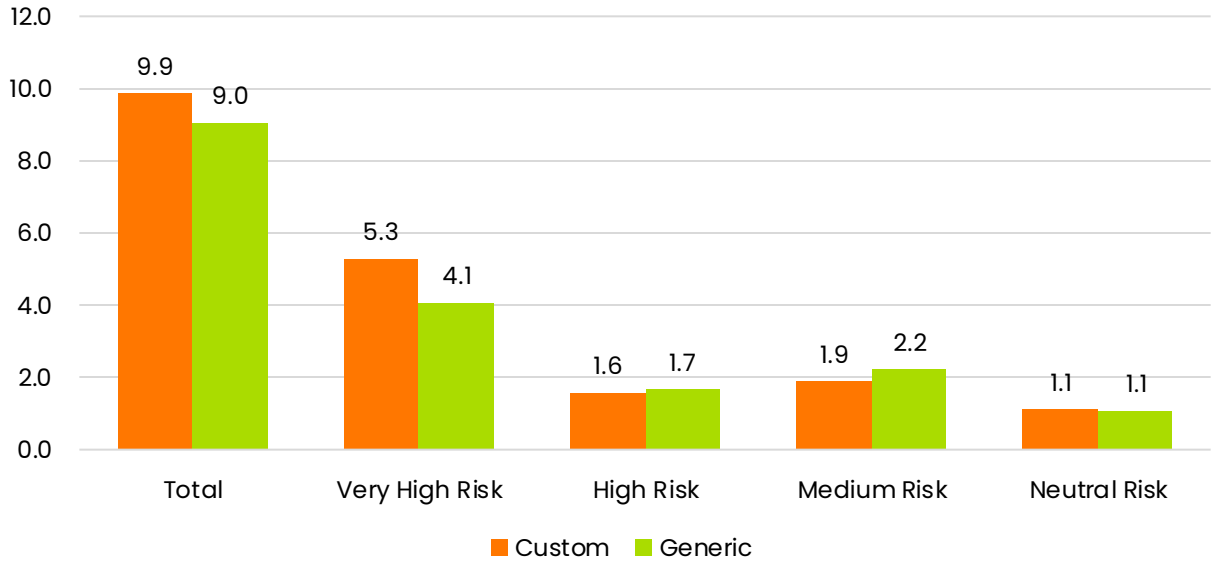
Figure 5.40 — Average # of SDKs - By OS



5.3.3.2 Average Number of SDKs per App by Generic vs. Custom

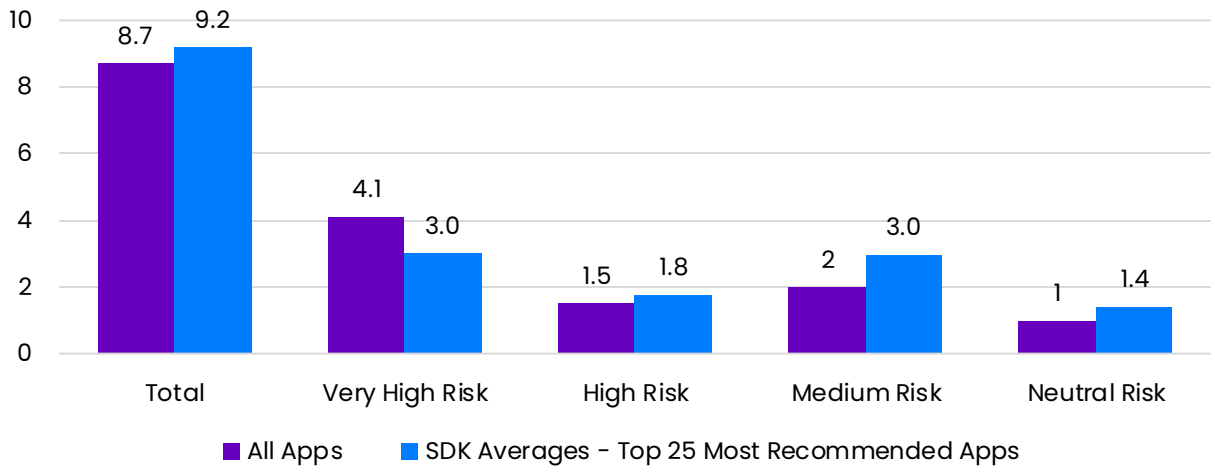
Custom apps have somewhat more SDKs on average than Generic apps. Similarly, Custom apps have on average more Very High Risk SDKs than generic apps.

Figure 5.41 — Average # SDKs - Custom/Generic



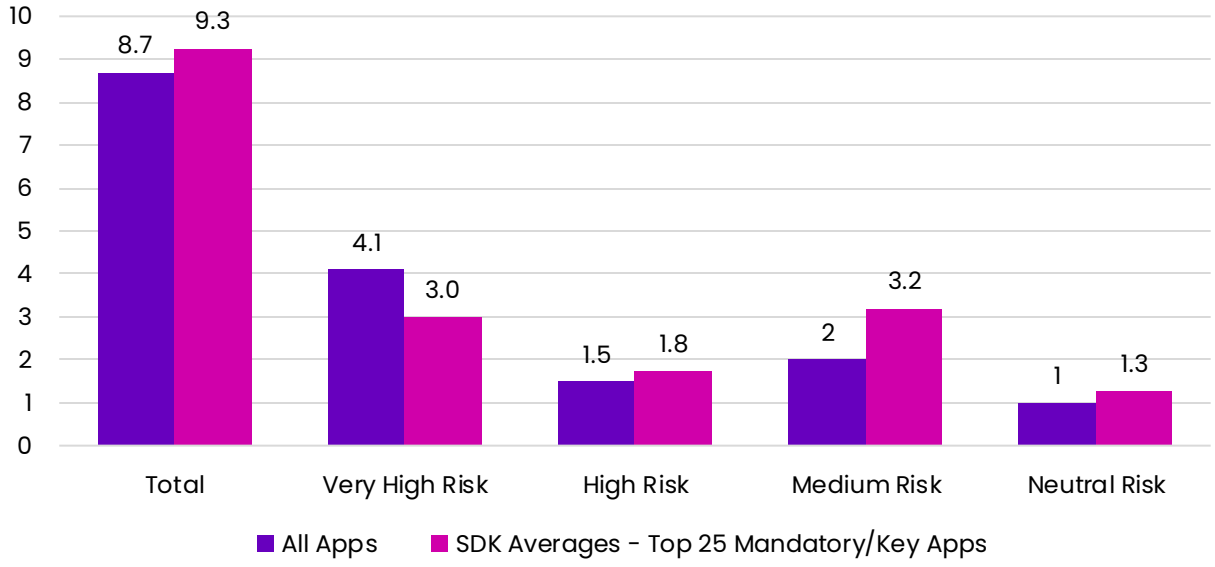
5.3.3.3 Average Number of SDKs Most Recommended Apps

Figure 5.42 — SDK Averages - 25 Most Recommended Apps



5.3.3.4 Average Number of SDKs Most Mandatory Apps

Figure 5.43 — SDK Averages - Top 25 Mandatory/Key Apps



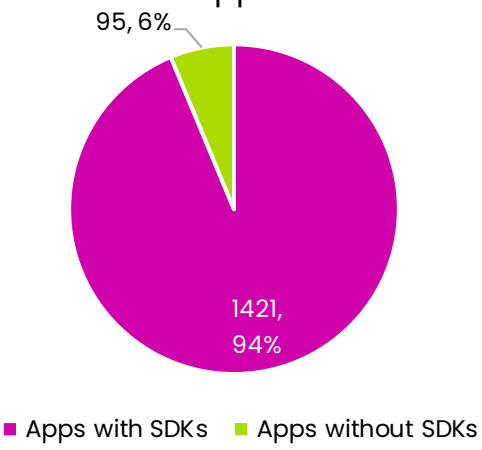
5.3.4 Apps with No SDKs

5.3.4.1 Apps with No SDKs Key Findings

- 94% of the apps studied have at least 1 SDK.
- 68% of the apps with no SDKs were iOS apps.

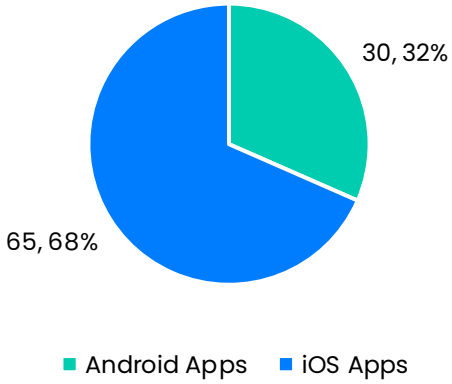
5.3.4.2 Apps with/without SDKs

Figure 5.44 — SDK Usage in Apps



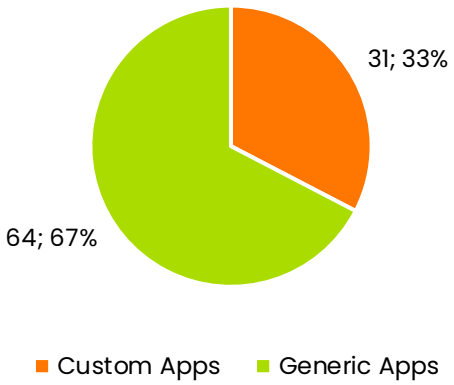
5.3.4.3 Apps with No SDKs by OS

Figure 5.45 — All Apps with no SDKs - By OS



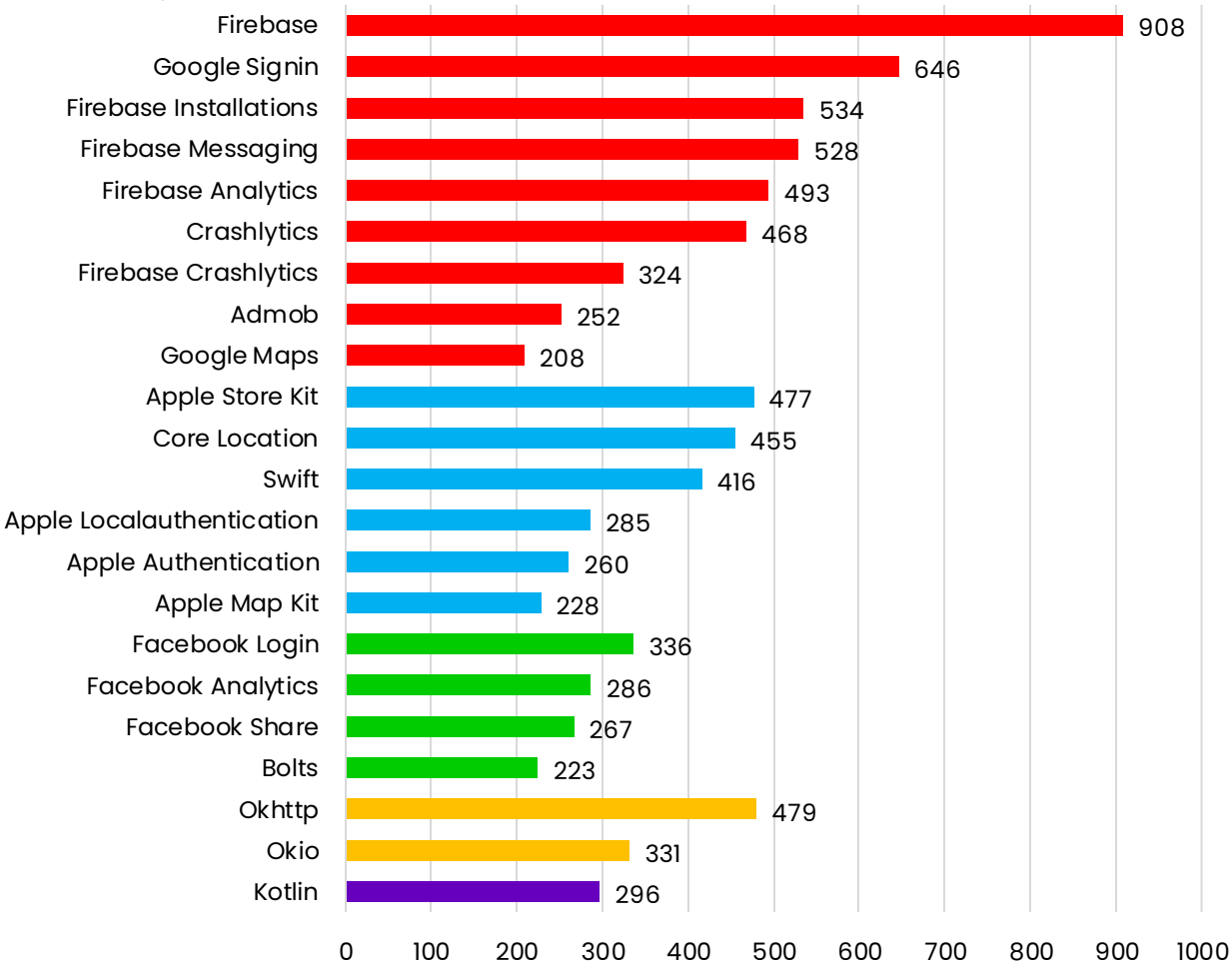
5.3.4.4 Apps with No SDKs – Custom vs. Generic

Figure 5.46 — Apps without SDKs - By Custom/Generic



5.3.5 Most Frequently Used SDKs (Clustered by Developer)

Figure 5.47 — Most Frequently Used SDKs (clustered by Developer)



5.3.6 Google and Apple SDKs

5.3.6.1 Apps with Google or Apple SDKs

- 70% of all the apps included Google SDKs, compared to 38% of all apps included Apple SDKs. This is mainly attributable to the fact that Android apps never include Apple SDKs, but Apple apps often include Android SDKs.
- 56.9% of the iOS apps in the sample included Google SDKs, and none of the Android apps included Apple SDKs.

Figure 5.48 — Apps Containing Google SDKs

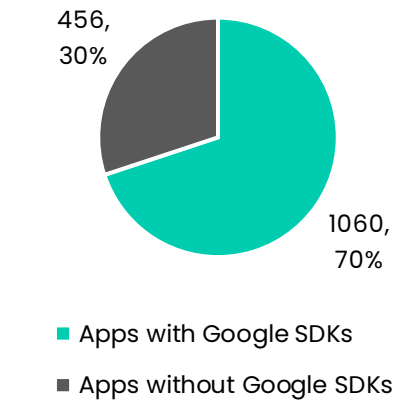


Figure 5.49 — Apps Containing Apple SDKs

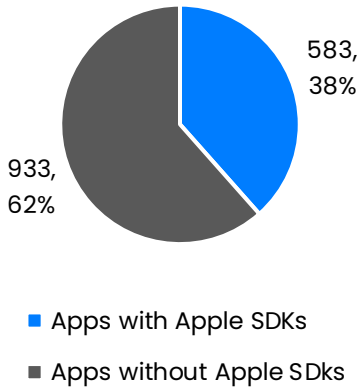


Figure 5.48a — Apps with Google SDKs by OS

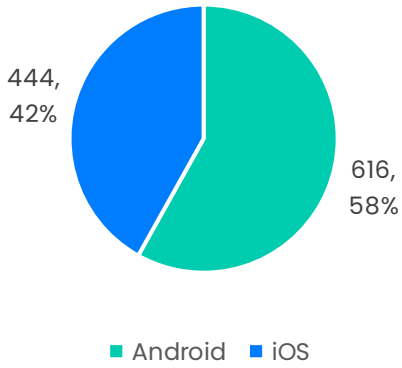
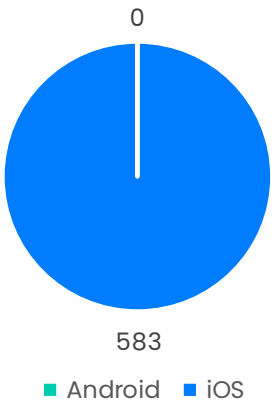


Figure 5.49a — Apps with Apple SDKs by OS



5.3.6.2 Apps with Google or Apple SDKs by OS and Custom vs. Generic

Figure 5.50 — Apps with Google SDKs

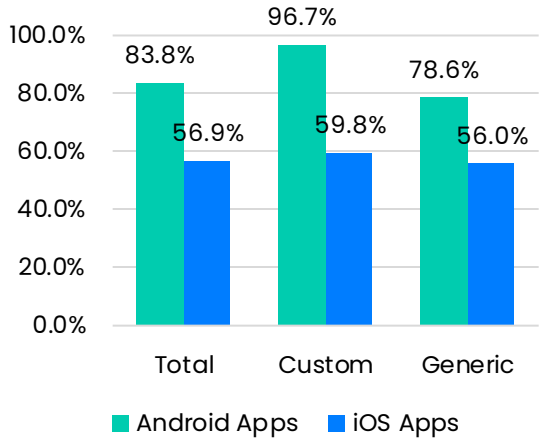
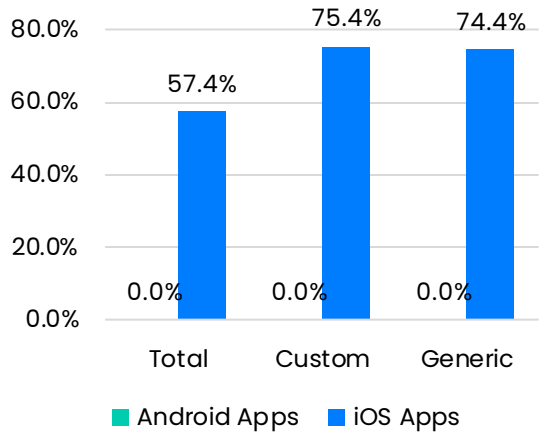


Figure 5.51 — Apps with Apple SDKs



5.3.7 SDK-based App Risk Profile Analysis

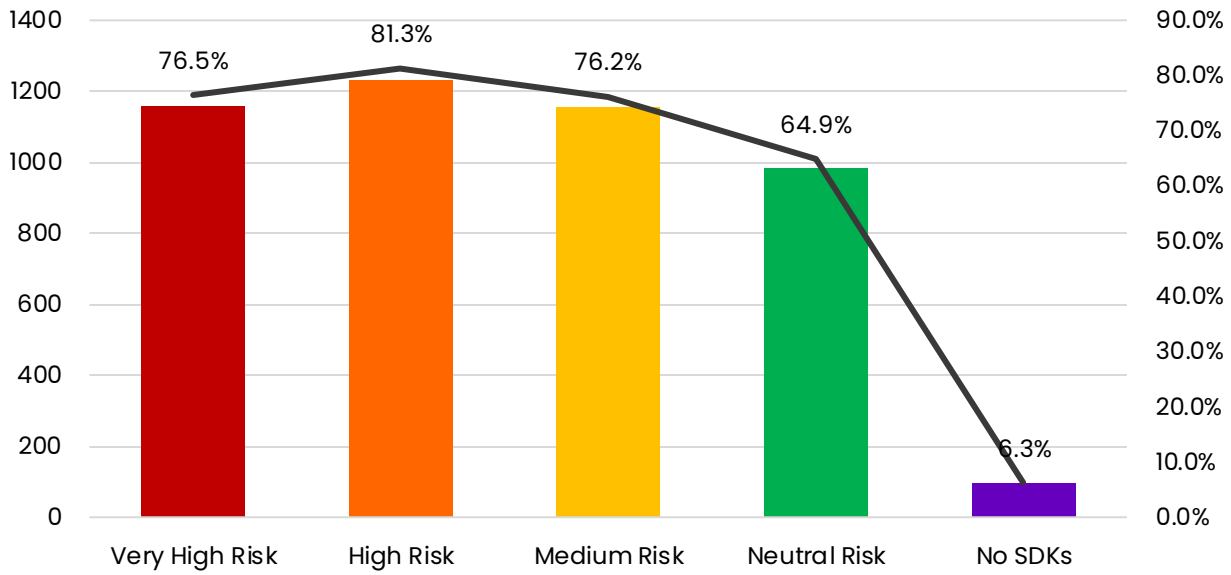
This section analyzes the risk profiles of apps that include SDKs. A risk profile is the overall percentages (likelihood) of SDKs by risk category for a given population of apps.

5.3.7.1 SDK-based App Risk Profile Key Findings

- **81.6%** of apps that had one or more SDK included **Very High Risk** SDKs.
- **86.7%** of apps that had one or more SDK included **High Risk** SDKs.
- Only **6.3%** of apps had **no** SDKs.
- Custom apps were somewhat more risky than Generic apps.
    - **86.6%** of **Custom** apps with SDKs had **Very High Risk** SDKs compared to **79.8%** of **Generic** apps.
    - **98.6%** of **Custom** apps with SDKs had **High Risk** SDKs compared to **82.8%** of **Generic** apps.
- **Android** apps were **significantly riskier** than **iOS** apps.
    - **89.9%** of **Android** apps include **Very High Risk** SDKs, compared to **iOS** apps' **63.6%**.
    - **84.1%** of **Android** apps include **High Risk** SDKs, compared to **iOS** apps' **78.6%.**
    - **iOS** apps include more **Medium Risk** SDKs (80.0%) than **Android** with **72.1%.**
- The most recommended apps were somewhat worse (higher) than the overall sample.
- The most frequently mandatory apps were also somewhat worse than both the most recommended apps and the overall sample.

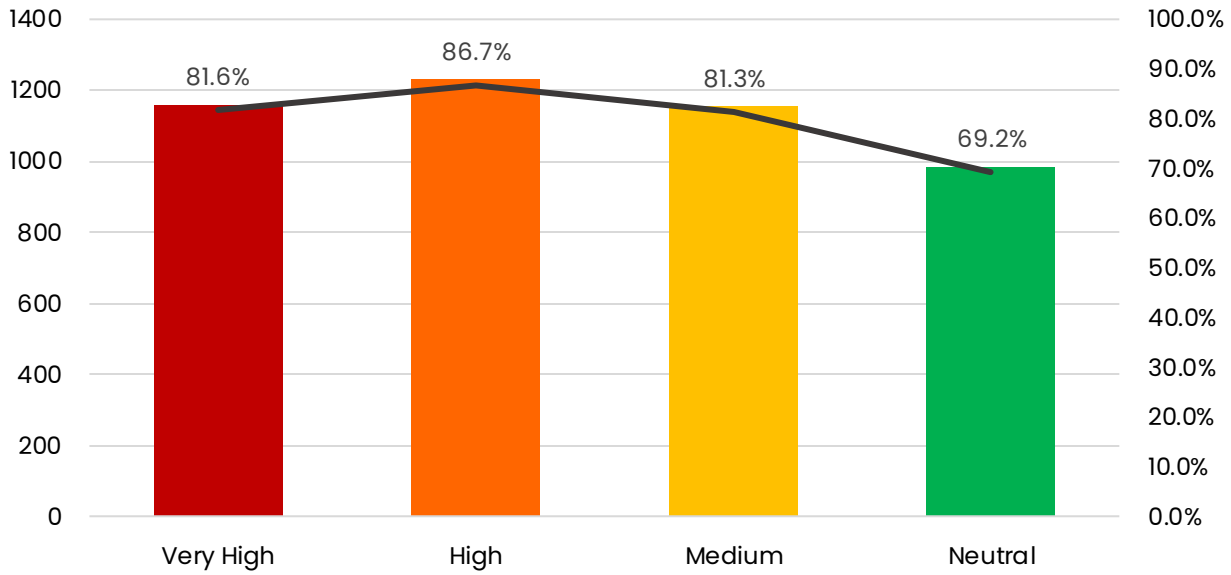
5.3.7.2 SDK-based App Risk Profile - All Apps

Figure 5.52 — SDK Risk Profile - All Apps



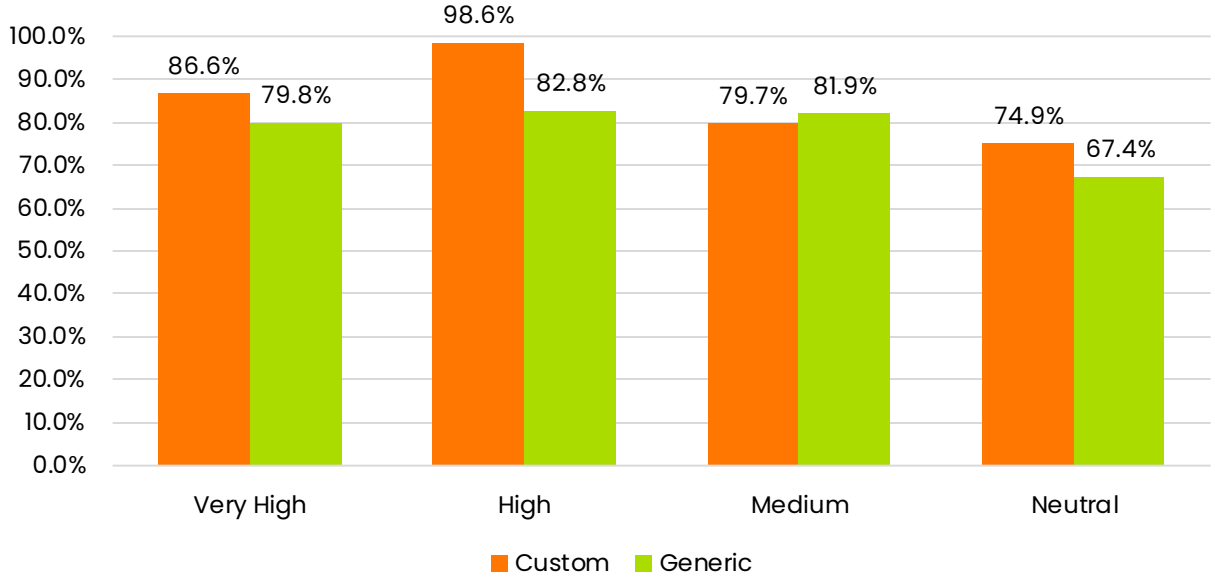
5.3.7.3 SDK-based Risk Profile – All Apps with SDKs

Figure 5.53 — SDK Risk Profile - Apps with SDKs



5.3.7.4 SDK-based Risk Profile – All Apps with SDKs] by Custom vs. Generic

Figure 5.54 — SDK Risk Profile - Custom vs. Generic



5.3.7.5 SDK-based Risk Profiles by Category

Figure 5.55 — Risk Profile - CEP Apps with SDKs

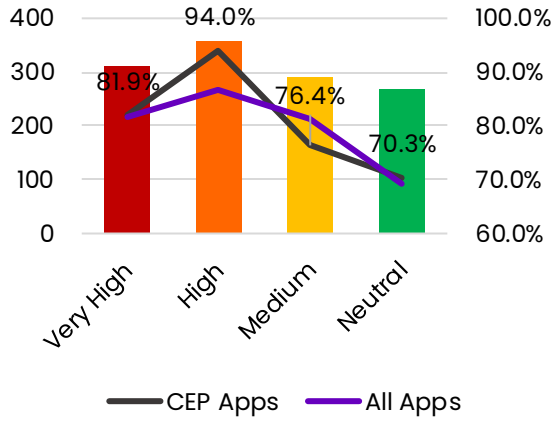


Figure 5.56 — Risk Profile - CMS Apps with SDKs

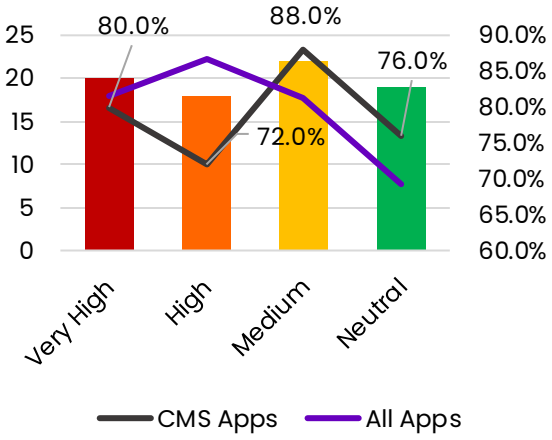


Figure 5.57 — Risk Profile - DLP Apps with SDKs

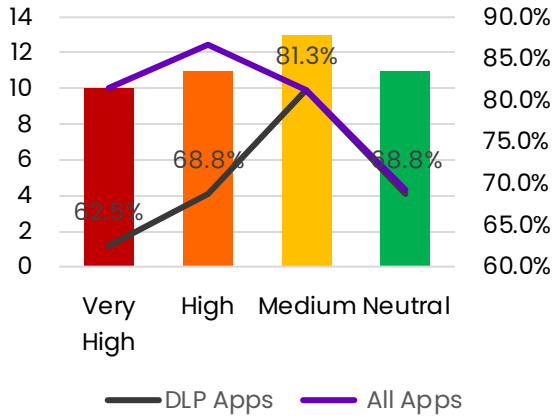


Figure 5.58 — Risk Profile - LeMS Apps with SDKs

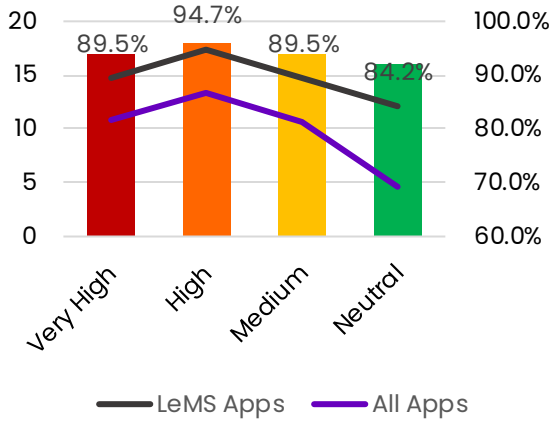


Figure 5.59 — Risk Profile - LiMS Apps with SDKs

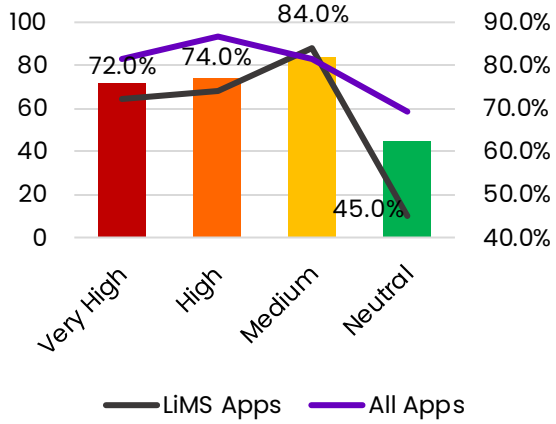


Figure 5.60 — Risk Profile - NES Apps with SDKs

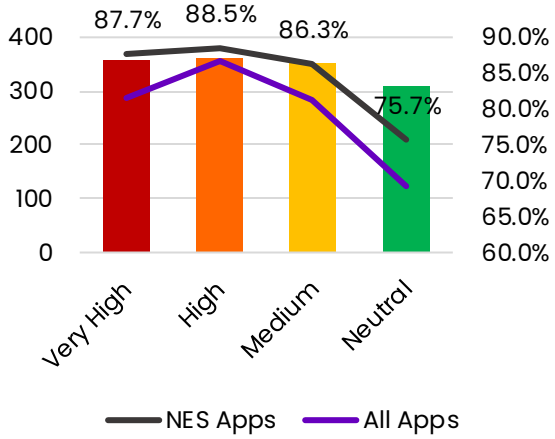


Figure 5.61 — Risk Profile - O Apps with SDKs

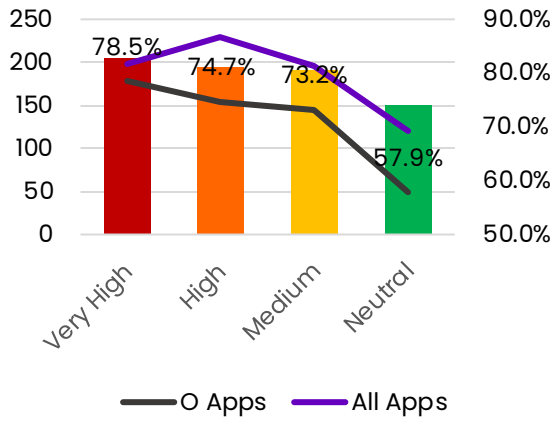


Figure 5.62 — Risk Profile - SIS Apps with SDKs

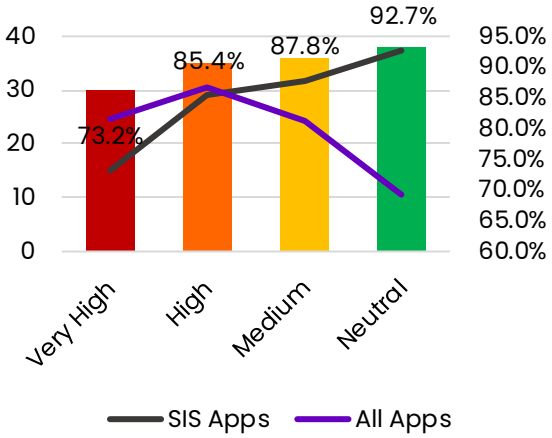


Figure 5.63 — Risk Profile - SMS Apps with SDKs

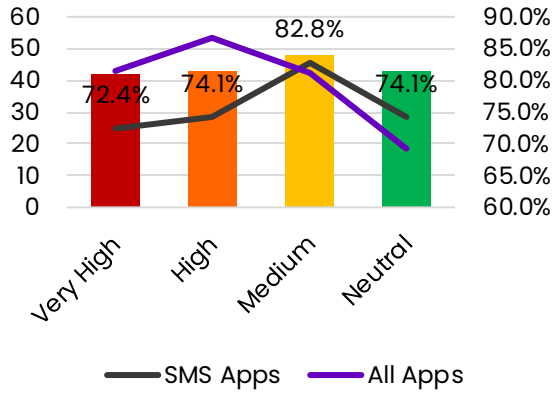


Figure 5.64 — Risk Profile - SP Apps with SDKs

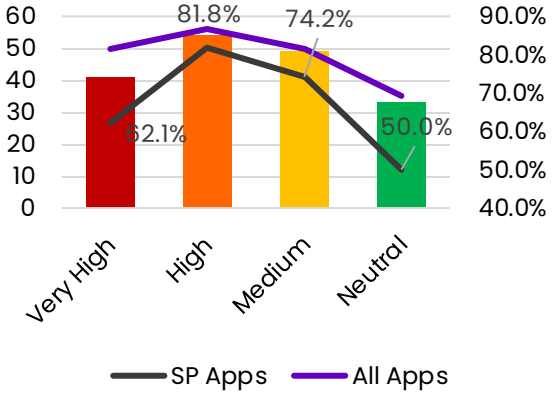


Figure 5.65 — Risk Profile - SSO Apps with SDKs

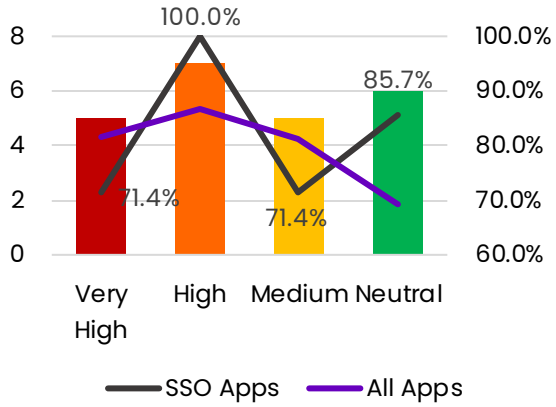


Figure 5.66 — Risk Profile - ST Apps with SDKs

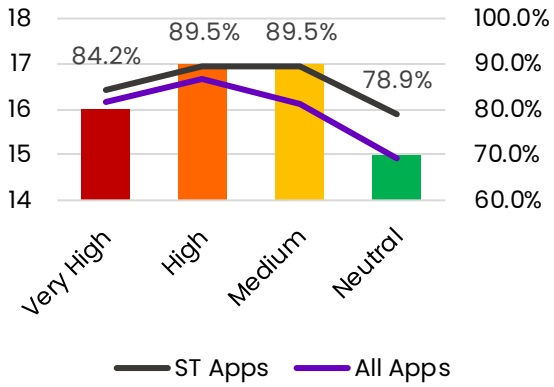


Figure 5.67 — Risk Profile - STS Apps with SDKs

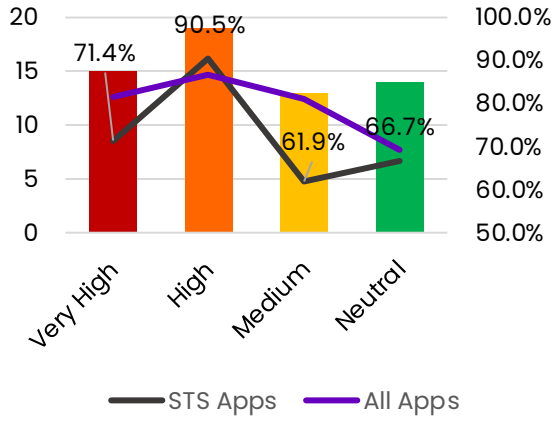
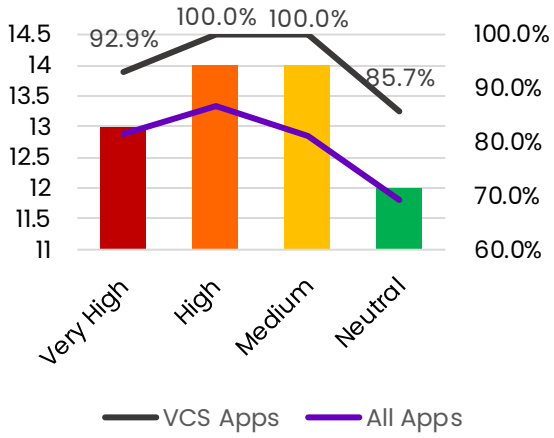
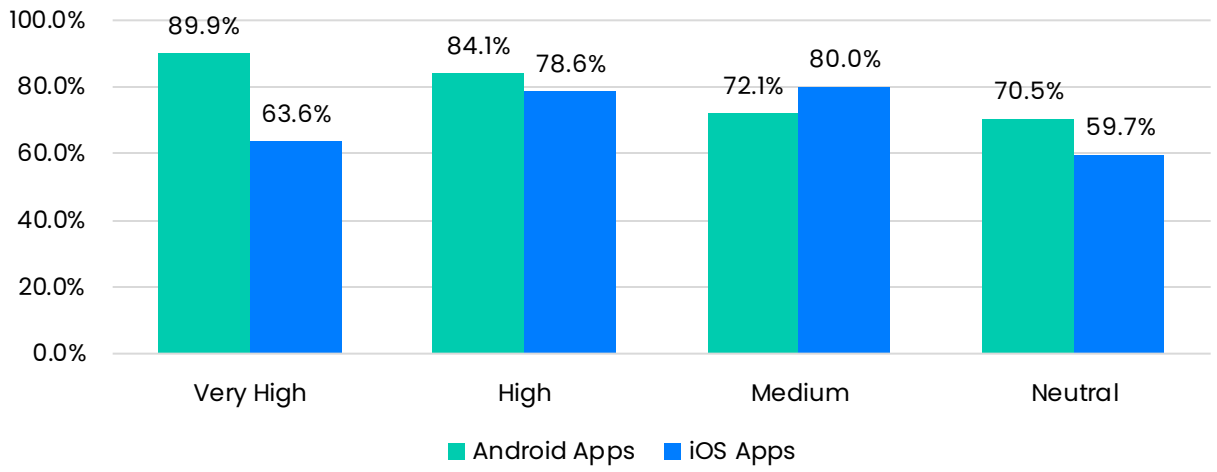


Figure 5.68 — Risk Profile - VCS Apps with SDKs



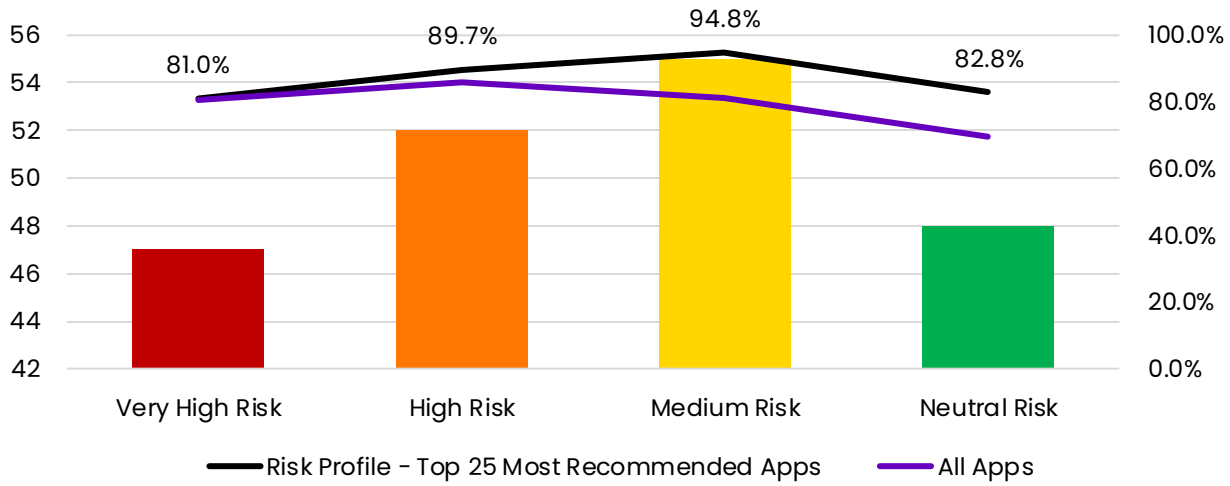
5.3.7.6 SDK-based Risk Profile – All Apps with SDKs by iOS vs. Android

Figure 5.69 — SDK Risk Profile - by OS



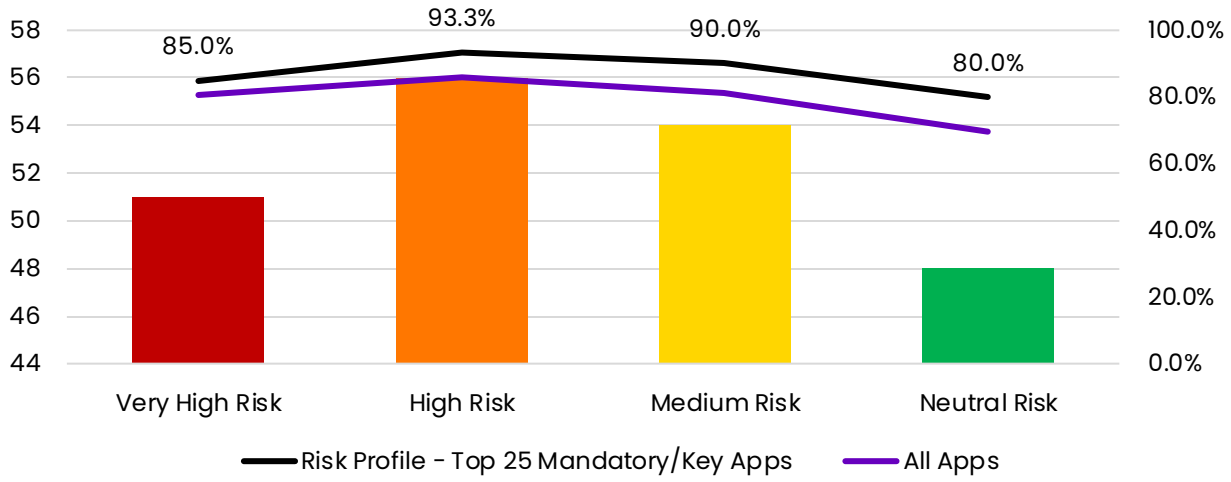
5.3.7.7 SDK-based Risk Profile – Most Recommended Apps

Figure 5.70 — Risk Profile - 25 Most Recommended Apps



5.3.7.8 SDK-based Risk Profile – Most Frequently Required Apps

Figure 5.71 — Risk Profile - Top 25 Mandatory/Key Apps



5.4 Permissions Analysis

To understand the kind of student information apps were accessing, we analyzed mobile app permissions. Mobile operating systems restrict access to features and data and allow apps to request access permissions. We classified the most common permission requests in terms of what risks they posed.

We classified iOS and Android sensitive permissions into seven buckets:

- **Location** includes any permission that potentially allows apps to determine the user's geographic location. Permissions such as wifi network names and bluetooth connections are included in this category because in many cases these names are distinctive and can be compared against databases to guess the location.
- **Files** include any permission that allows apps to list user data files or their contents, whether in the cloud or on device. This access is risky both because files and filenames can include personal information and because it can be used to fingerprint and reidentify a user even if they have reset other identifiers.
- **Join User Identifiers** includes any permission that directly assists advertising networks that wish to track users across apps or across device, such as with Apple's ID for Advertising (IDFA).
- **Physical Environment** includes permissions that reveal information about the user's physical environment, such as through camera and microphone.

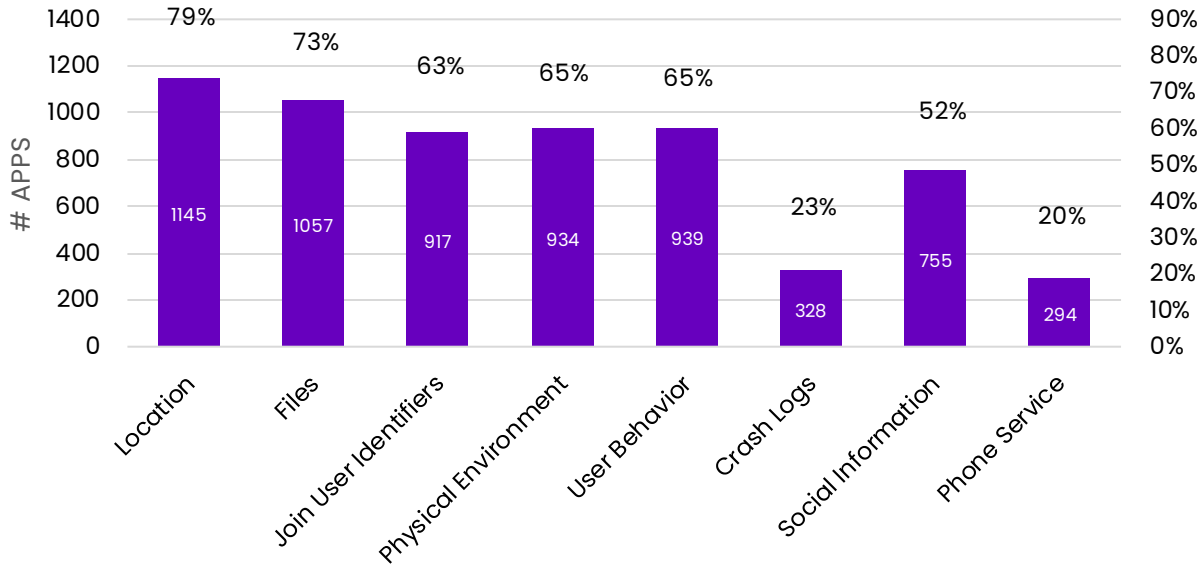
- **User Behavior** permissions include anything that would be useful to advertising networks seeking to learn more about a user, such as their psychology or interests.
- **Crash Logs** include permissions that allow the app publisher to receive information when the app crashes. There is a risk of this information including personal details.
- **Social Information** includes permissions that reveal who the user associates with, as well as when or where they do so. This includes calendar and contacts.
- **Phone Service** includes permissions that reveal who the user's carrier is or whether they currently have service. This can serve as a proxy for location. It may also reveal financial wellbeing.

5.4.1 Permissions Key Findings

- **Location**-related permissions were the most frequently occurring permission, appearing in **79%** of all apps.
- **73%** of apps requested **Files** access.
- **65%** of apps requested **Physical Environment** permissions such as camera and microphone access.
- **65%** of apps requested **User Behavior** permissions.
- **52%** of apps requested access to **Social Information**.
- Custom vs. Generic apps:
  - More **Custom** apps accessed key permissions than the overall apps.
    - **81%** of **Custom** apps accessed **Location Information**.
    - **69%** of **Custom** apps accessed **Social Information**.
  - Generic apps generally accessed key permissions in line with the overall app dataset.
- iOS vs. Android apps:
  - **100%** of **Android** apps requested **Location** permissions**.**
  - **Android** apps requested permissions **more** frequently than **iOS** apps except for:
    - **Physical Location: 73%** of **iOS** apps compared to **56%** of **Android** apps**.**
    - **Crash Logs**: **46**% of **iOS** apps compared to **0%** of **Android** apps.
    - **Social Information: 61%** of **iOS** apps compared to **43%** of **Android** apps**.**

5.4.2 Permissions – All Apps

Figure 5.72 — Permissions - All Apps



5.4.3 Permissions – Custom vs Generic Apps

Figure 5.73 — Permissions - Custom Apps

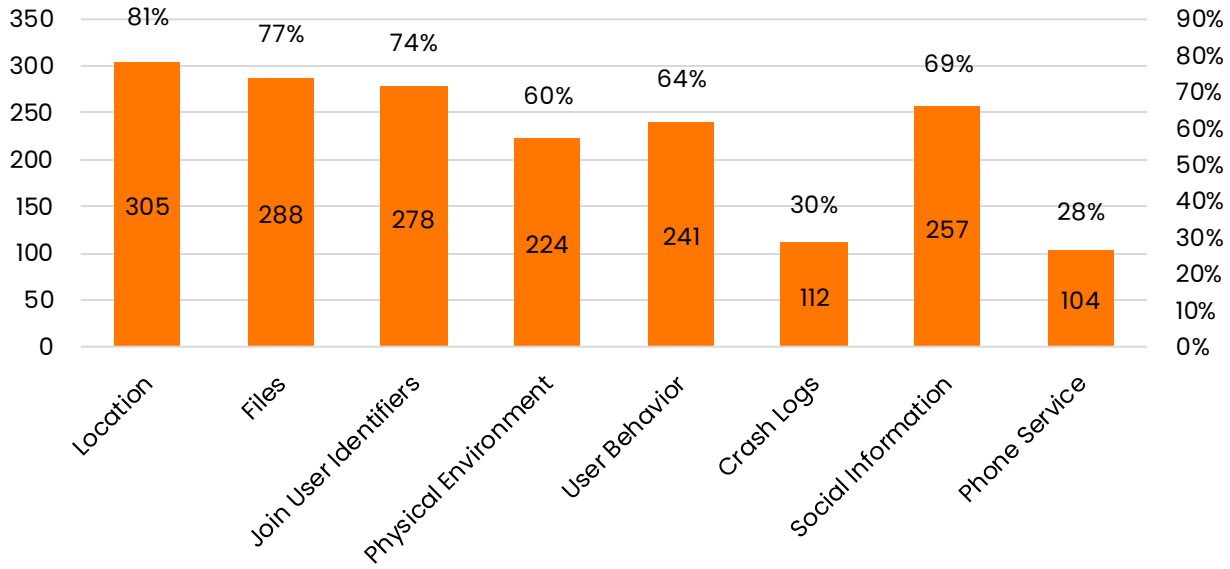
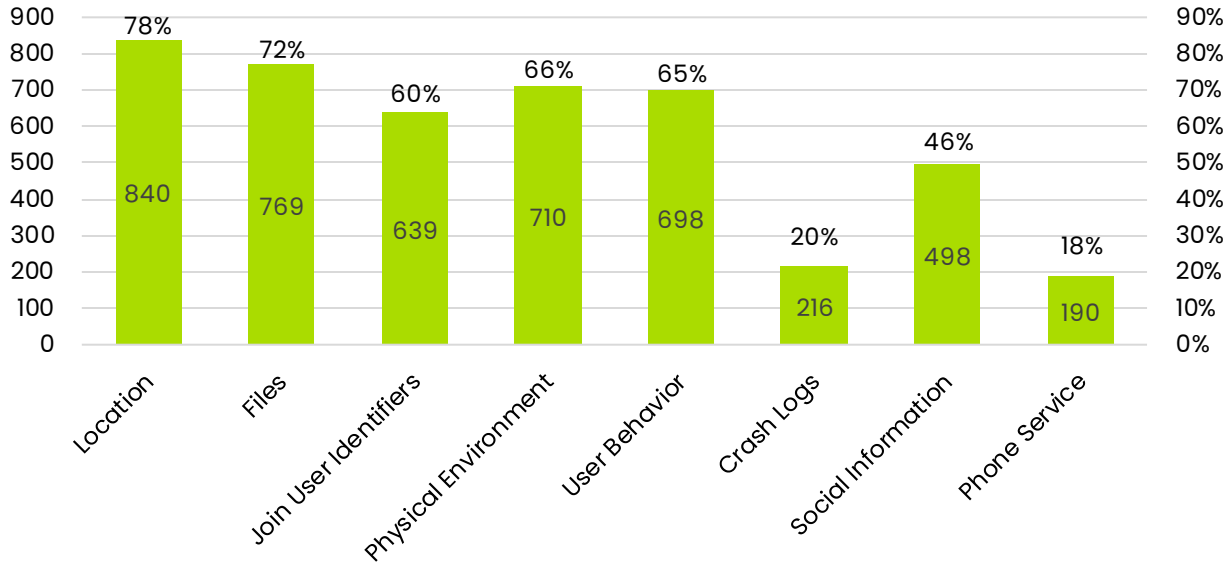


Figure 5.74 — Permissions - Generic Apps



5.4.4 Permissions by Category

The charts in this section convey how each category of apps compares to the permission behavior of the overall dataset. The intention is to try to characterize which categories have proclivities towards certain types of data.

Appendix D contains the permission summaries per category.

Figure 5.75 — % of Apps with Location Permissions by Category

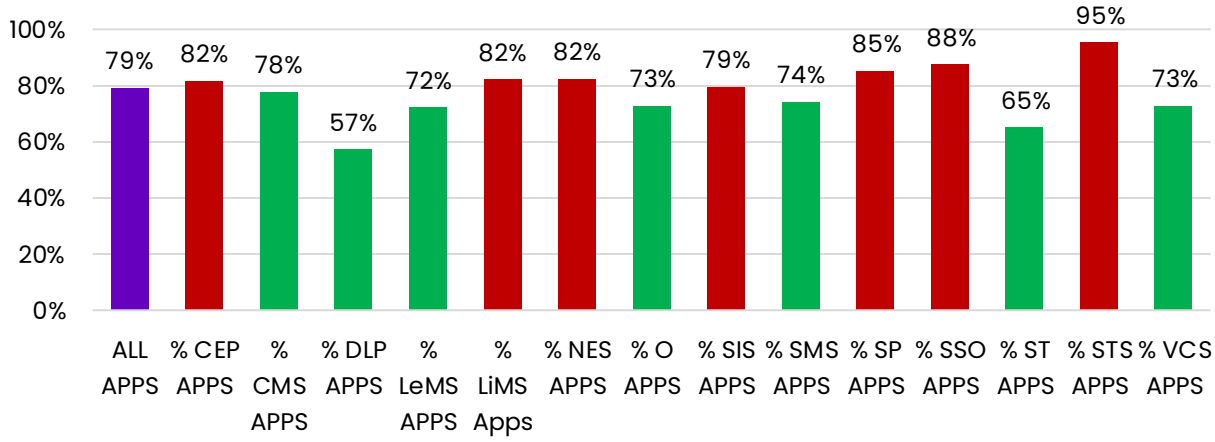


Figure 5.76 — % of Apps with Files Permissions by Category

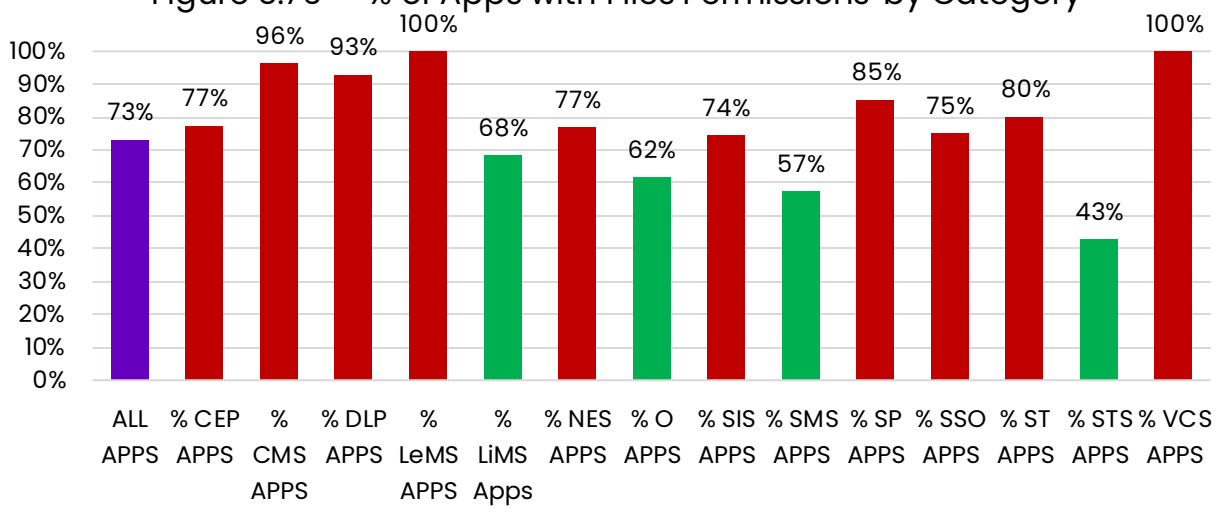


Figure 5.77 — % of Apps with Join User Identification Permissions by Category

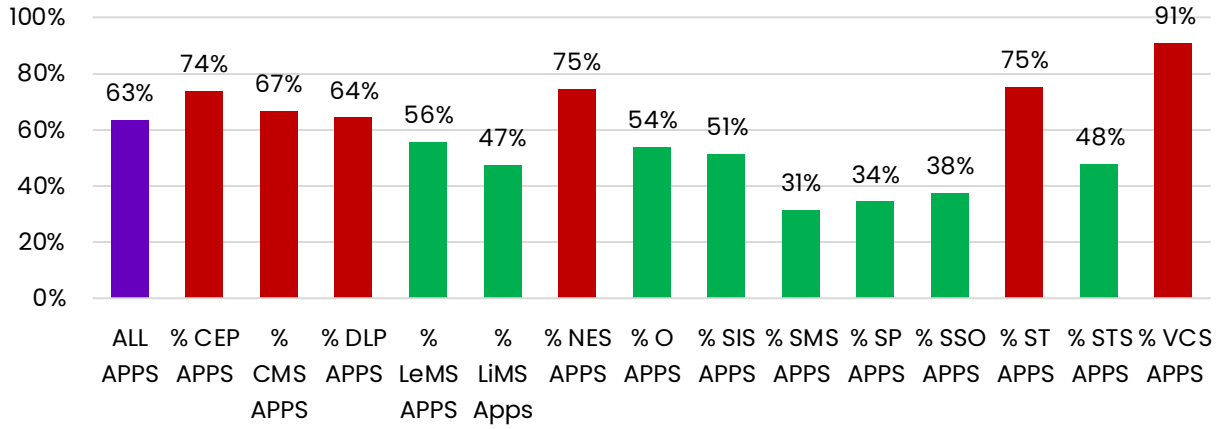


Figure 5.78 — % of Apps with Physical Environment Permissions by Category

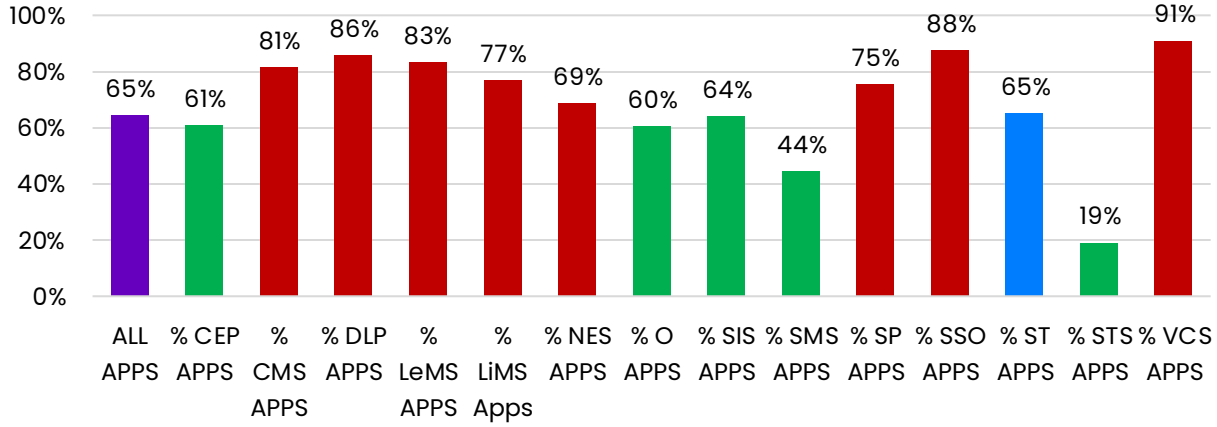


Figure 5.79 — % of Apps with User Behavior Permissions by Category

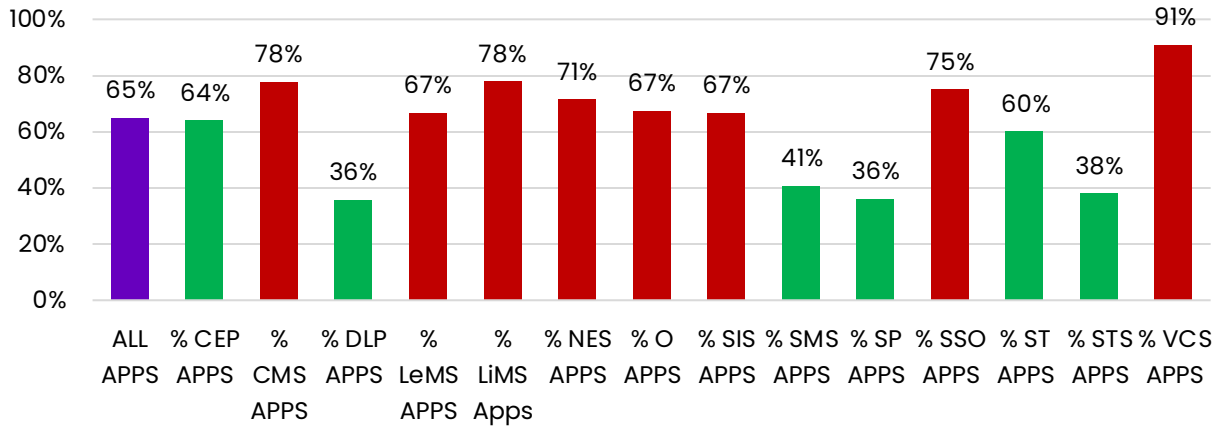


Figure 5.80 — % of Apps with Social Information Permissions by Category

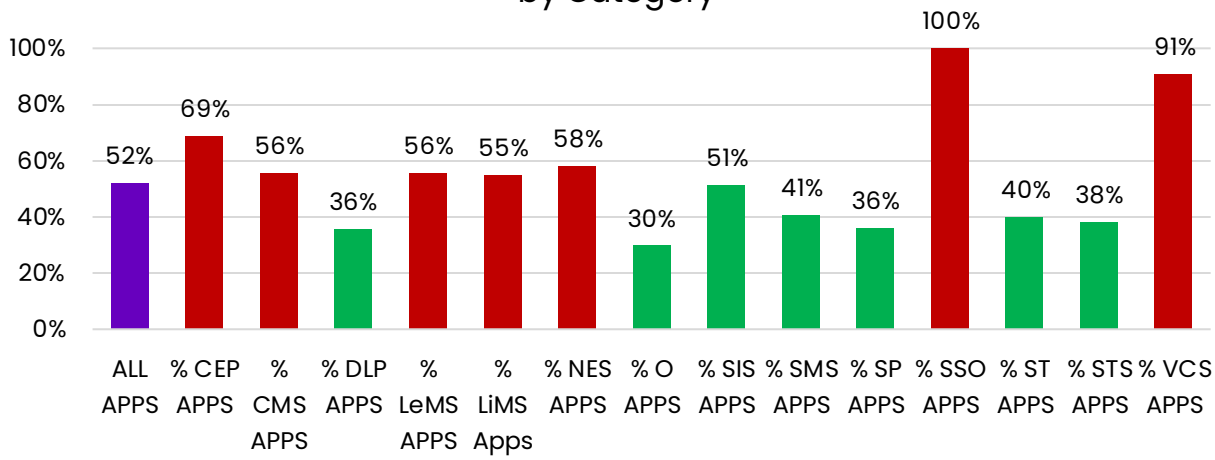
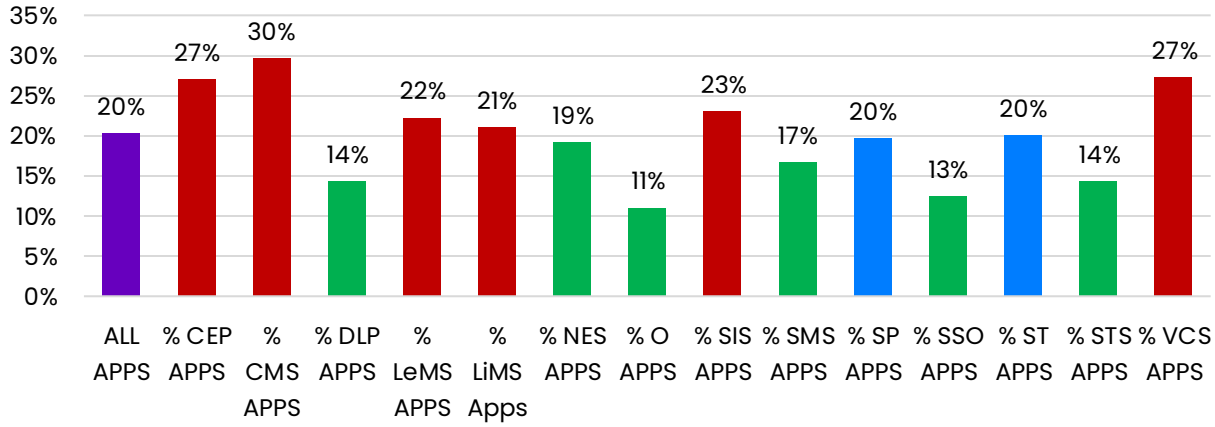


Figure 5.81 — % of Apps with Phone Service Permissions by Category



5.4.5 Permissions – iOS vs Android

Figure 5.82 — Permissions - iOS Apps

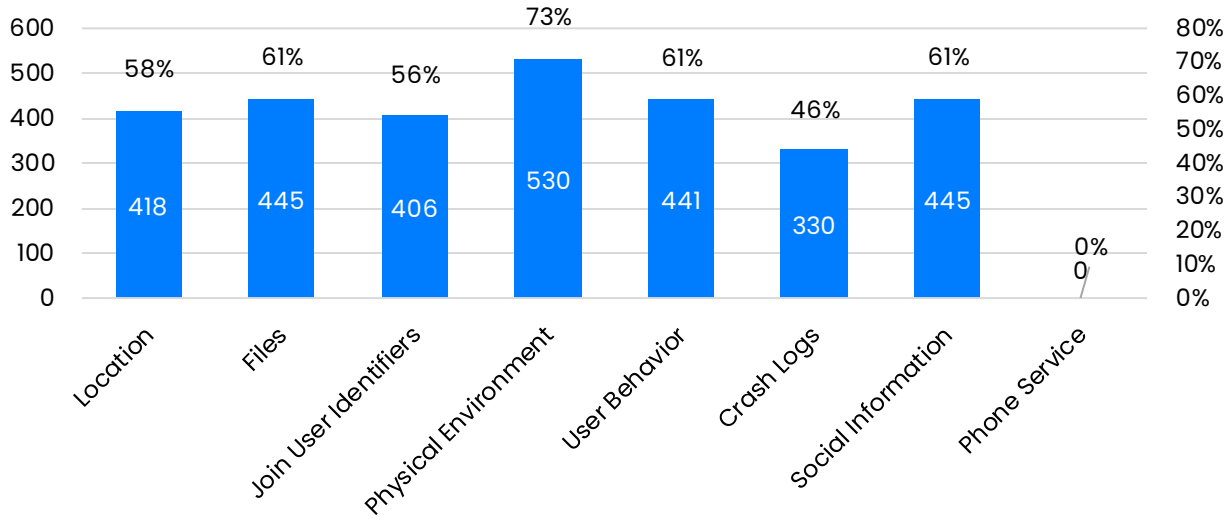
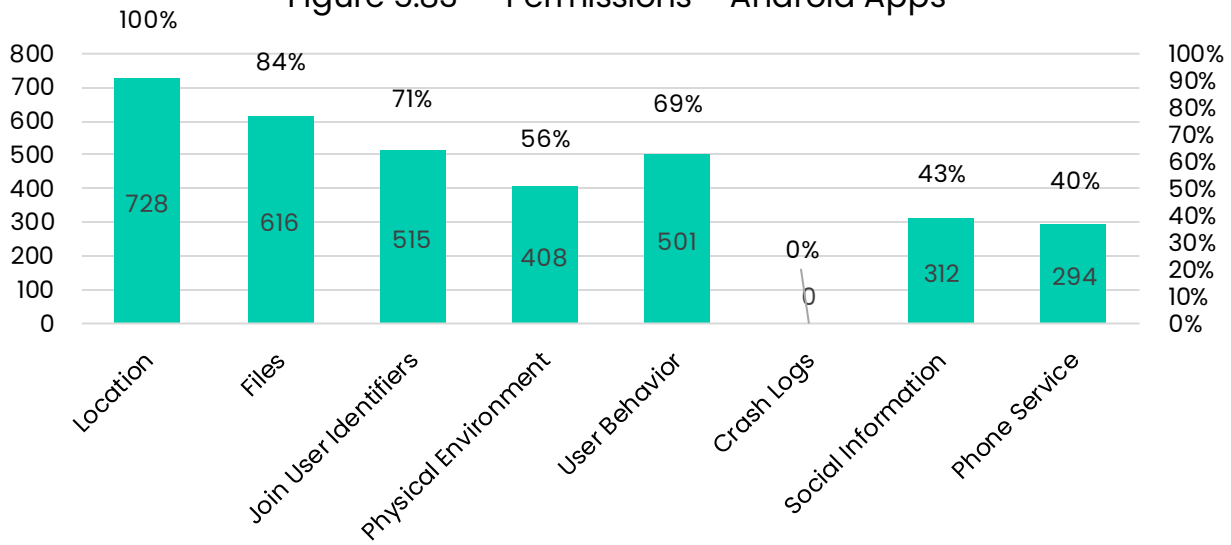
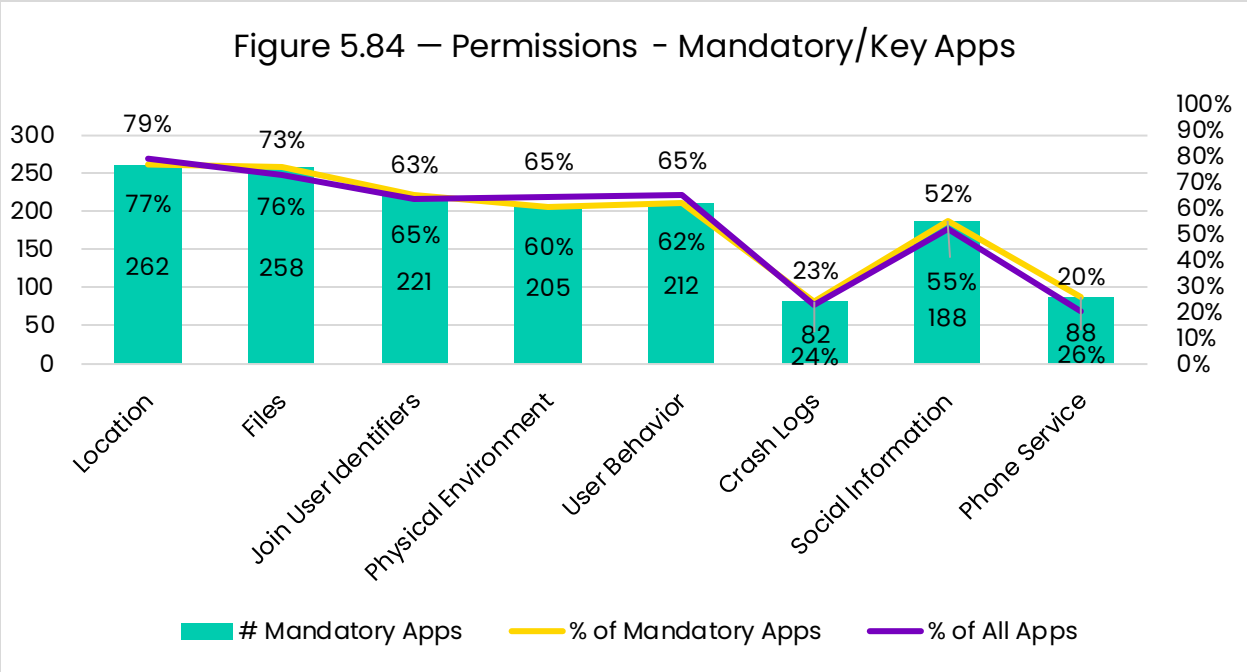


Figure 5.83 — Permissions - Android Apps



5.4.6 Permissions – Most Required Apps



5.5 Advertising Analysis

This section describes the advertising behaviors observed in the testing of the apps. We looked for two things:

1. Any type of advertising—indicating that adtech was being utilized to populate advertising area within the app, and
2. Retargeting advertising in particular, namely ads that were personalized based on browser history or other personal information.

Both behaviors are dangerous to children and should not exist in apps being used by children, as they both result in personally identifying information being sent into the vast adtech network. Retargeting advertising is significantly worse, as it implies that more of the child's information is being sent to the adtech network, which Is why it's been banned for students in 25 states.[4]

We also observed "sponsorship" ads that appeared to be hard-coded local sponsorships (similar to what is found in school yearbooks). We tracked instances of those separately, as they do not represent the safety risk that traditional digital ads do.

[4] "The State Student Privacy Report Card", p. 8, Parent Coalition for Student Privacy, January 2019. https://t8bb96.a2cdn1.secureserver.net/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf

It should be noted that It's very likely that the ad presence and retargeting ad presence numbers are lower than the actual ad presence, since these were tagged only when observed by our researchers in the course of manually testing the app.

5.5.1 Advertising Key Findings

- **23%** of all tested apps **included advertising**. This is a much larger than desired amount of advertising.
- **13%** of all tested apps included **retargeting personalized advertising**.
- Custom and Generic apps behaved largely the same, **except there were more retargeting ads in generic apps.**
- If we remove the non-education specific (NES) apps, the percent of tested apps with ads drops to 18% and the percent of apps with retargeting ads drops to 9%. Still too high to be safe for students.
- iOS vs. Android:
  - There was no appreciable difference between the platforms with respect to ad presence. This speaks to the fact that both platforms can yield safe apps.

Figure 5.85 — Ad Presence - All Apps

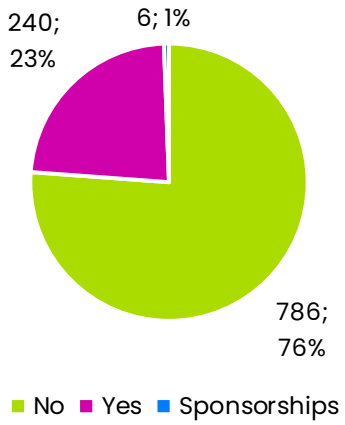


Figure 5.86 — Ad Presence - Custom Apps

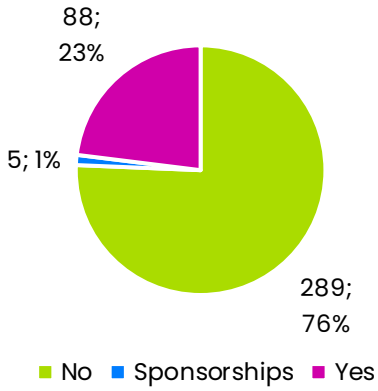


Figure 5.87 — Ad Presence - Generic Apps

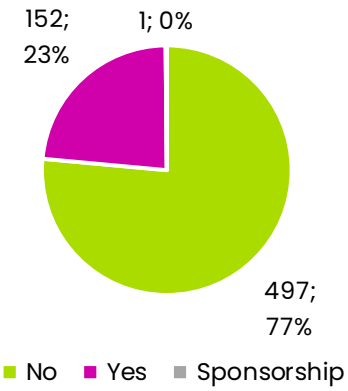


Figure 5.88 — Retargeting Ad Presence - All Apps

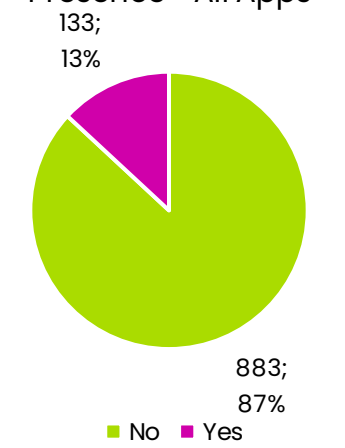


Figure 5.89 — Retargeting Ad Presence - Custom Apps

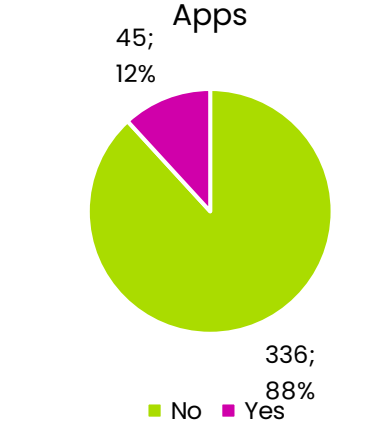
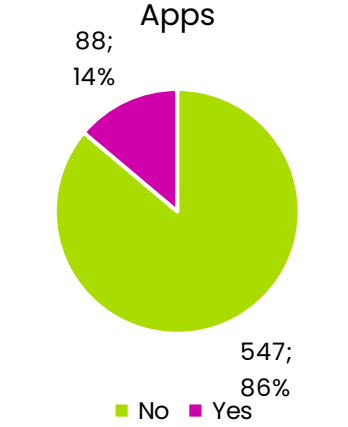


Figure 5.90 — Retargeting Ad Presence - Generic Apps



5.5.2 Ad Presence Excluding Non-Education Specific (NES) Apps

Non-education specific apps contained the most retargeted ads, and we wanted to see the behavior across everything but the NES apps.

Figure 5.91 — Ad Presence Total - Excluding NES

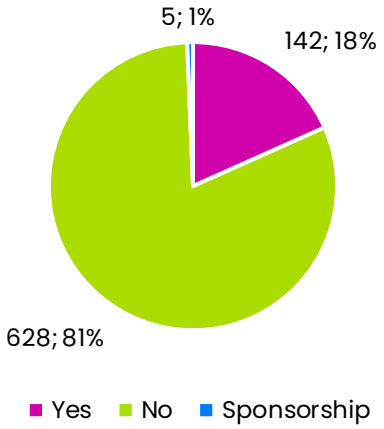
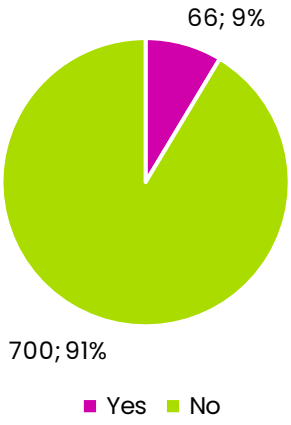


Figure 5.92 — Retargeting Ad Presence - Excluding NES

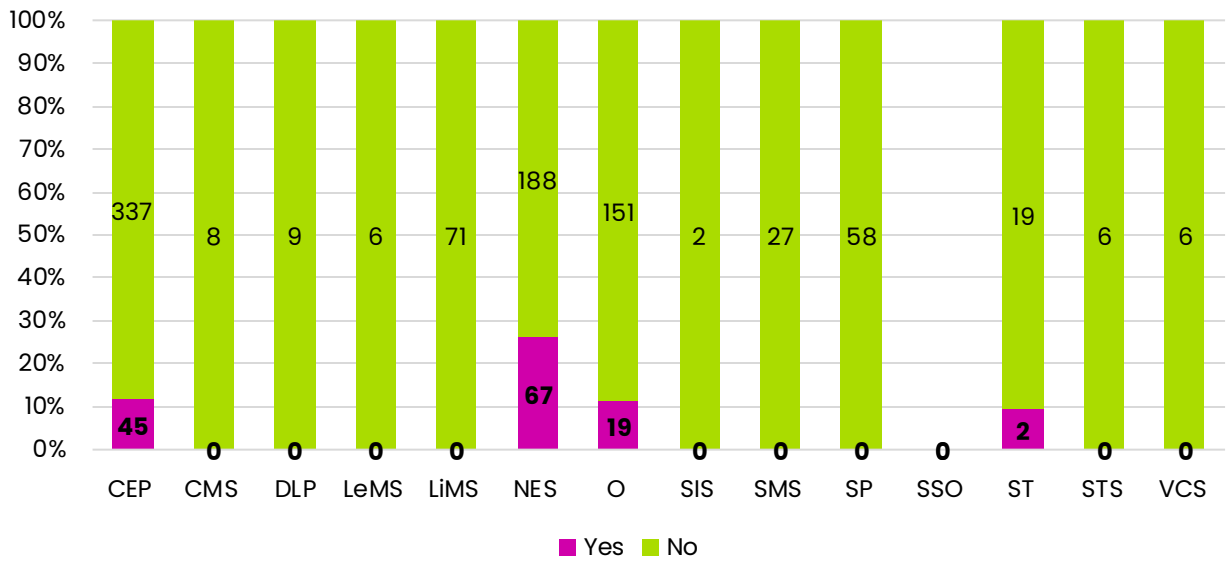


5.5.3 Ad Presence by App Category

Figure 5.93 — Ad Presence by App Category

5.5.1 Retargeting Ad Presence by App Category

Figure 5.94 — Retargeting Ad Presence by App Category



5.5.2 Ad Presence by OS

Figure 5.95 — Ad Presence in Android Apps

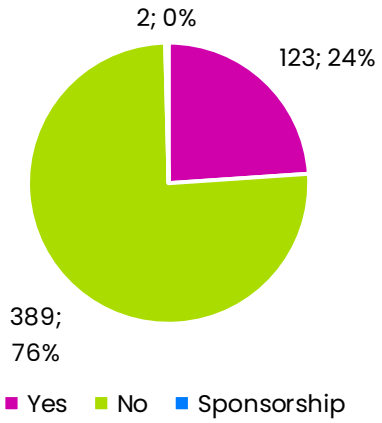
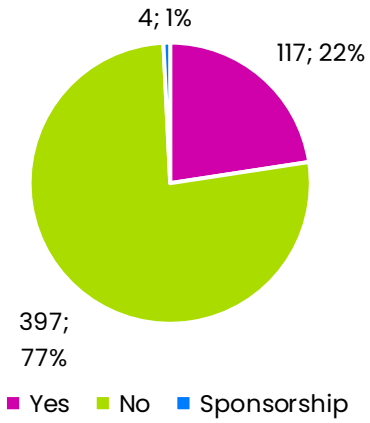


Figure 5.96 — Ad Presence in iOS Apps



5.5.3 Retargeting Ad Presence by OS

Figure 5.97 — Retargeting Ad Presence in Android Apps

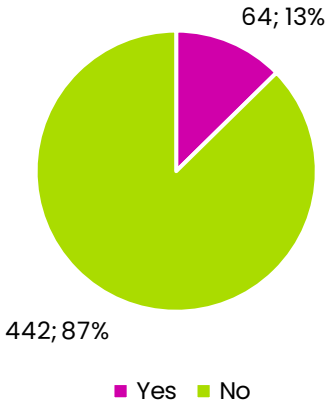
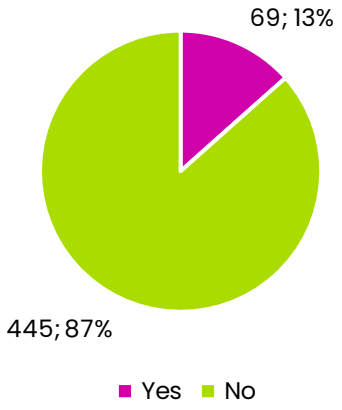


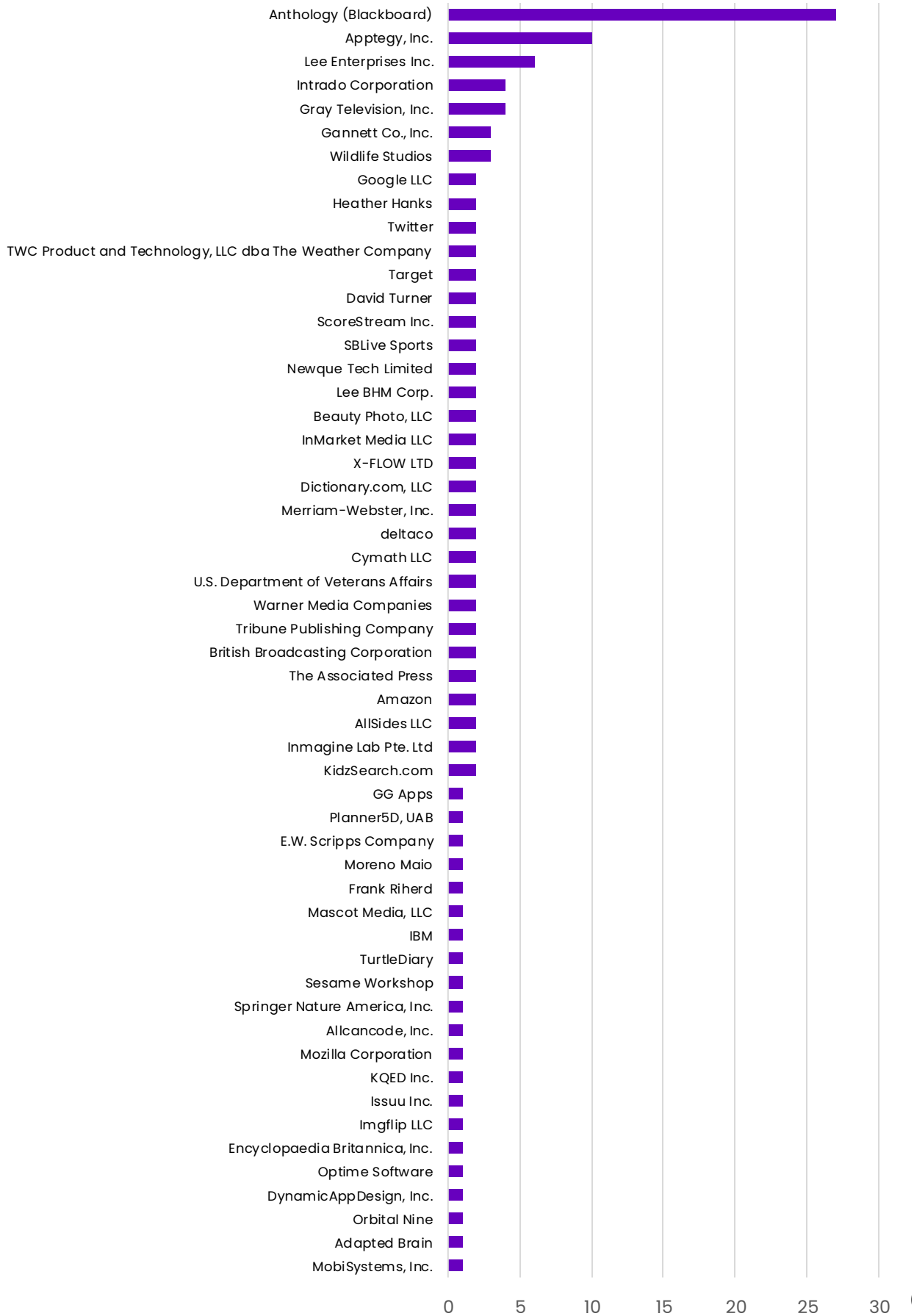
Figure 5.98 — Retargeting Ad Presence in iOS Apps



5.5.4 Developers with Observed Retargeting Ads

Figure 5.98a below shows the developers with observed retargeting ads in the apps. Many of these apps are not strictly for children, so the presence of retargeting ads isn't overly surprising. However, there are noteworthy K12 edtech developers including Blackboard and Apptegy. We also compiled the full list of apps that had retargeting ads In Appendix E. Note that the list of apps includes several CES type apps, a "COVID Coach" app, a math skills app, and several coloring book apps, which are among the least safe apps.

Figure 5.98a — Developers of Apps with Observed Retargeting Ads



5.6 Data Sharing with Large Platforms Analysis

As mentioned earlier, in this report we recorded network traffic on all testable apps. For this report, we are including findings on observed data sent to six of the largest platforms, specifically:

- Adobe
- Amazon
- Apple
- Facebook
- Google
- Twitter

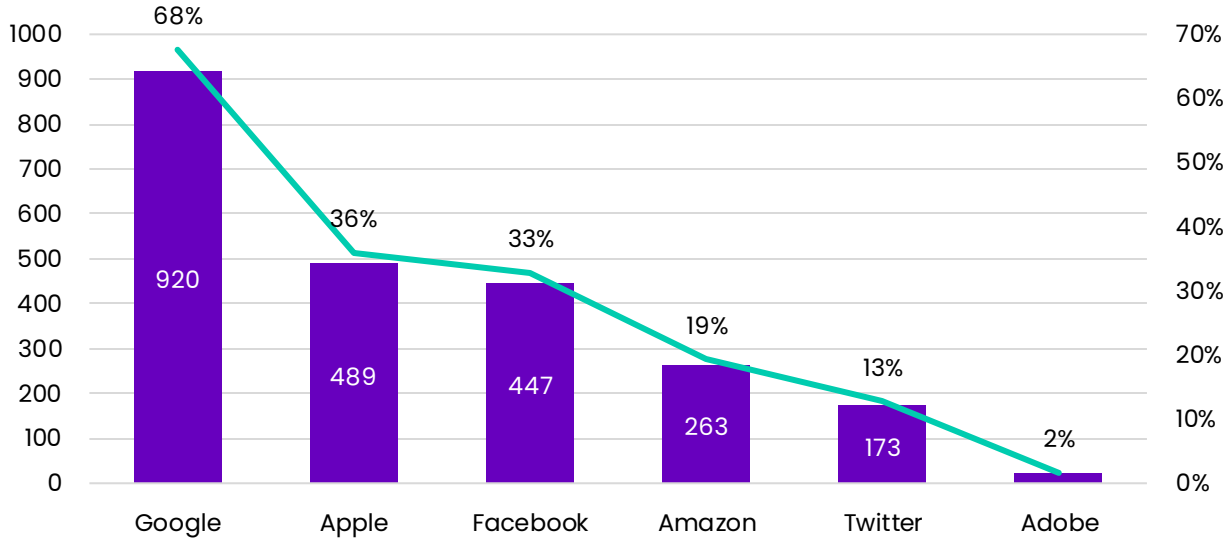
5.6.1 Platform Data Sharing Key Findings

- **68% of tested apps sent data to Google**
- 36% of tested apps sent data to Apple
- 33% of tested apps sent data to Facebook
- **34% of tested apps sent data to 3 or more of the 6 platforms.**
- **11% of tested apps sent data to 5 of 6 platforms.**
- Custom vs. Generic Apps:
    - Generic apps had more traffic to:
        - Google (71%) than Custom apps (61%)
        - Apple (40%) than Custom apps (26%).
        - Adobe (2%) than Custom apps (1%)
    - Custom apps had more traffic to:
        - Facebook (41%) than Generic apps (30%)
        - Amazon (27%) than Generic apps (16%)
        - Twitter (25%) than Generic apps (8%)
    - **61% of Custom apps were observed sending data to Google, significantly higher than the 49% of apps as reported in Spotlight Report #1.**
- By Category:
    - 45% of Study Tool (ST) apps and 40% of Community Engagement Platforms (CEP) apps sent data to Facebook.
    - The Study Tool (ST) category of apps sent more data to Amazon, Apple, Facebook, Google and Twitter than any other category (as a % of apps).
- iOS vs. Android:
    - **iOS apps more frequently sent data to all six large platforms than Android apps.**
- Most recommended and most frequently required apps:
    - **None** of the tested most recommended or most frequently required apps had traffic to **Amazon** or **Twitter.**

- **Only 2%** of tested most **required** and **3%** of most **recommended** apps sent traffic to **Facebook.**
- Google**:**
  - **80%** of tested most frequently **required** apps sent data to **Google.**
  - **68%** of tested most **recommended** apps sent data to **Google.**
- Apple**:**
  - **35%** of tested most frequently **required** apps sent data to **Apple.**
  - **30%** of tested most **recommended** apps sent data to **Apple**

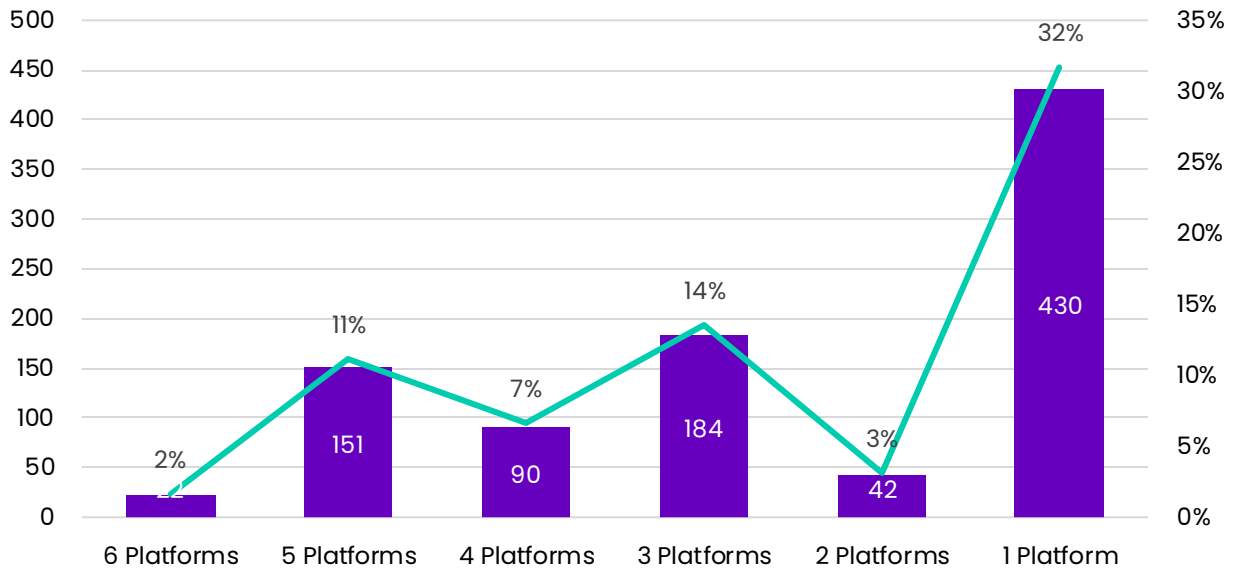
5.6.2 Platform Data Sharing - All Apps

Figure 5.99 — Observed Network Traffic to Platforms - All Apps, as % of tested apps



5.6.3 Platform Data Sharing Frequency

Figure 5.100 — # Platforms Observed



5.6.4 Platform Data Sharing - Custom vs. Generic Apps

Figure 5.101 — Observed Network Traffic to Platforms - Custom Apps, as % of apps

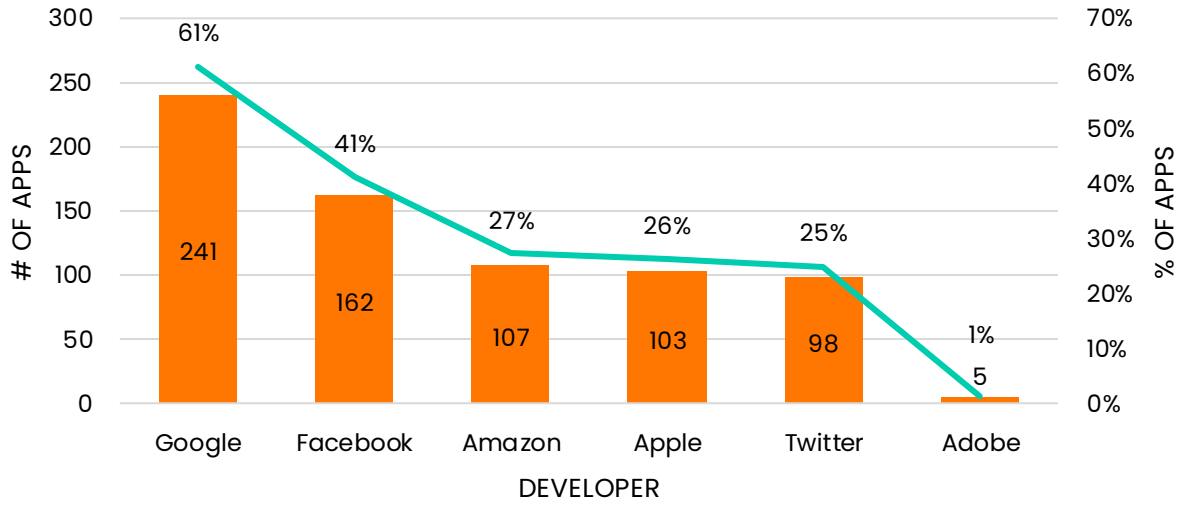
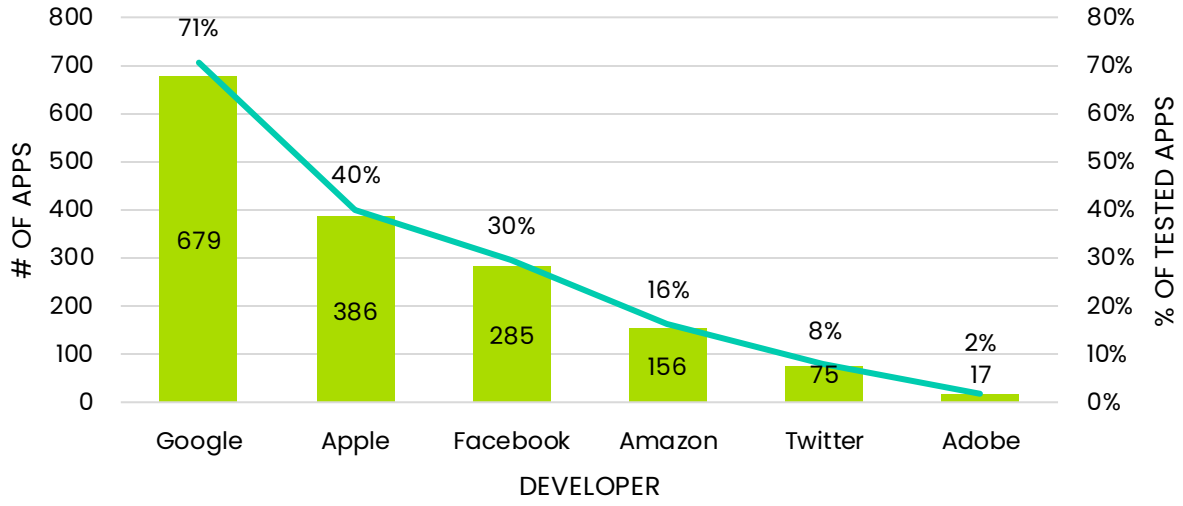


Figure 5.102 — Observed Network Traffic to Platforms - Generic Apps, as % of tested apps



5.6.5 Platform Data Sharing – by App Category

Figure 5.103 — # Apps with NW Traffic to Adobe by Category

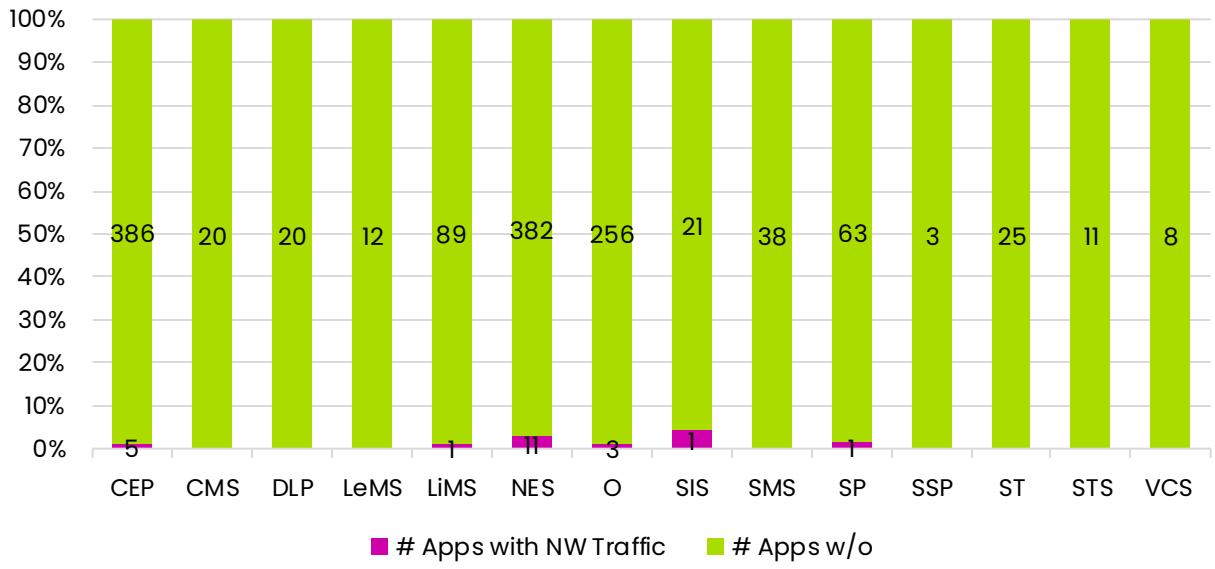


Figure 5.104 — # Apps with NW Traffic to Amazon by Category

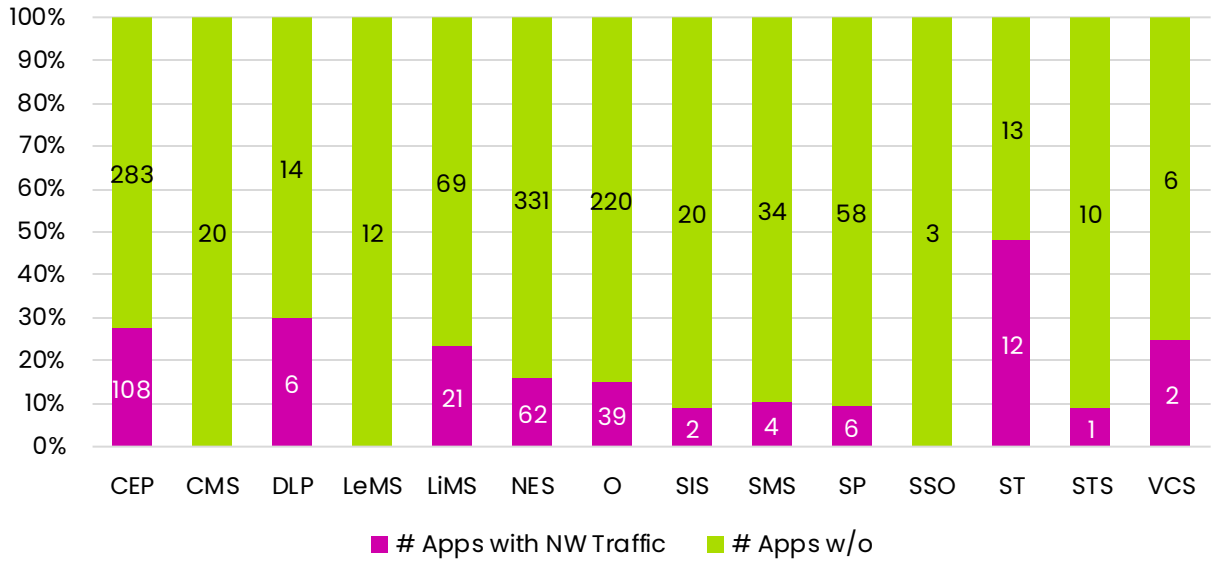


Figure 5.105 — # Apps with NW Traffic to Apple by Category

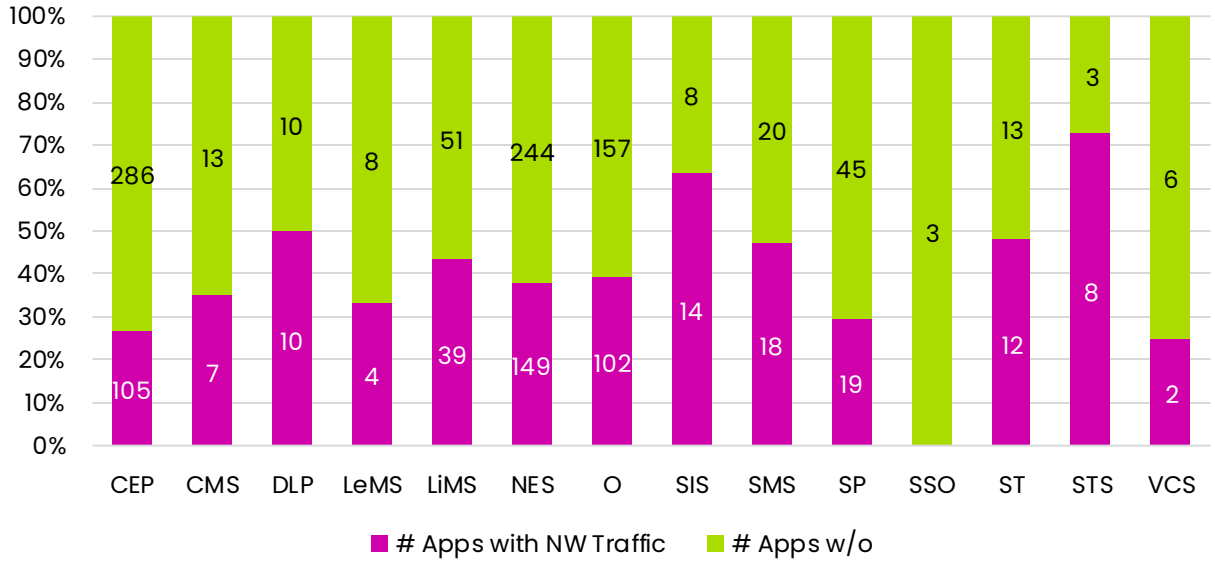


Figure 5.106 — # Apps with NW Traffic to Facebook by Category

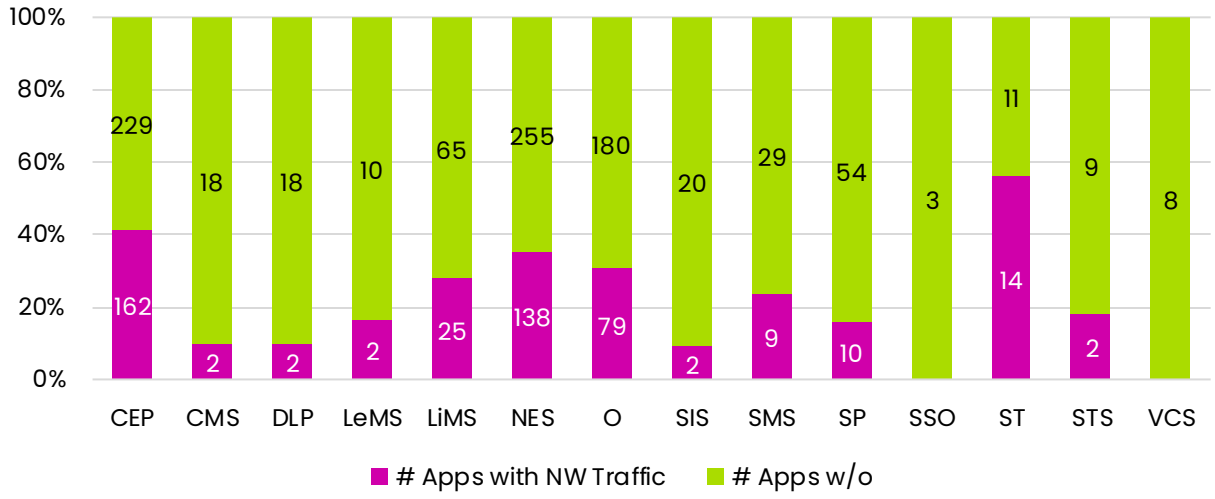


Figure 5.107 — # Apps with NW Traffic to Google by Category

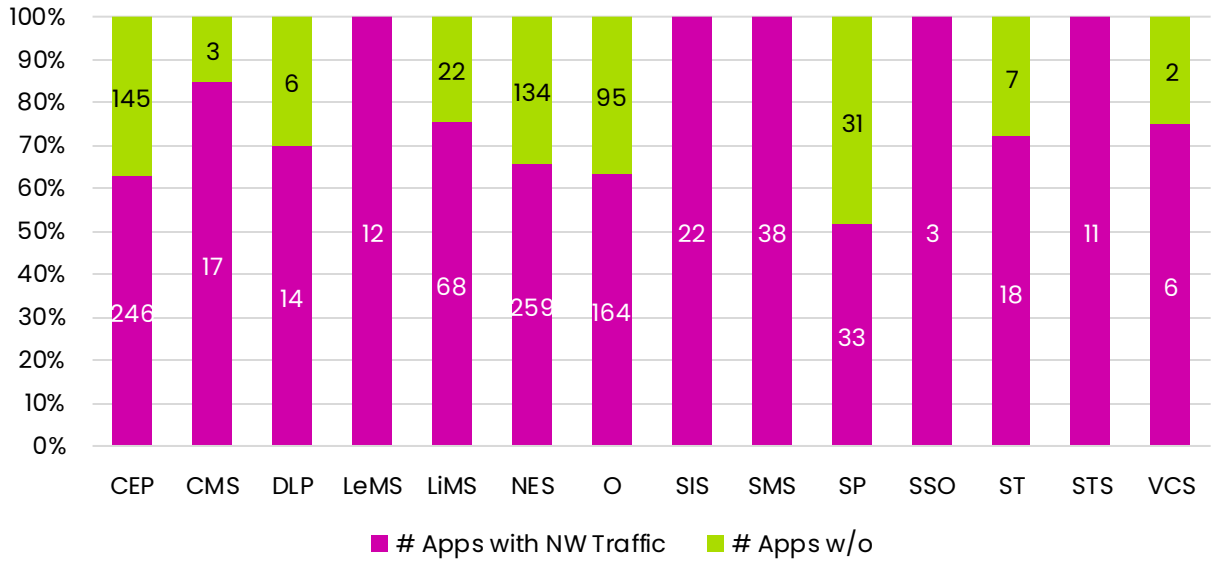
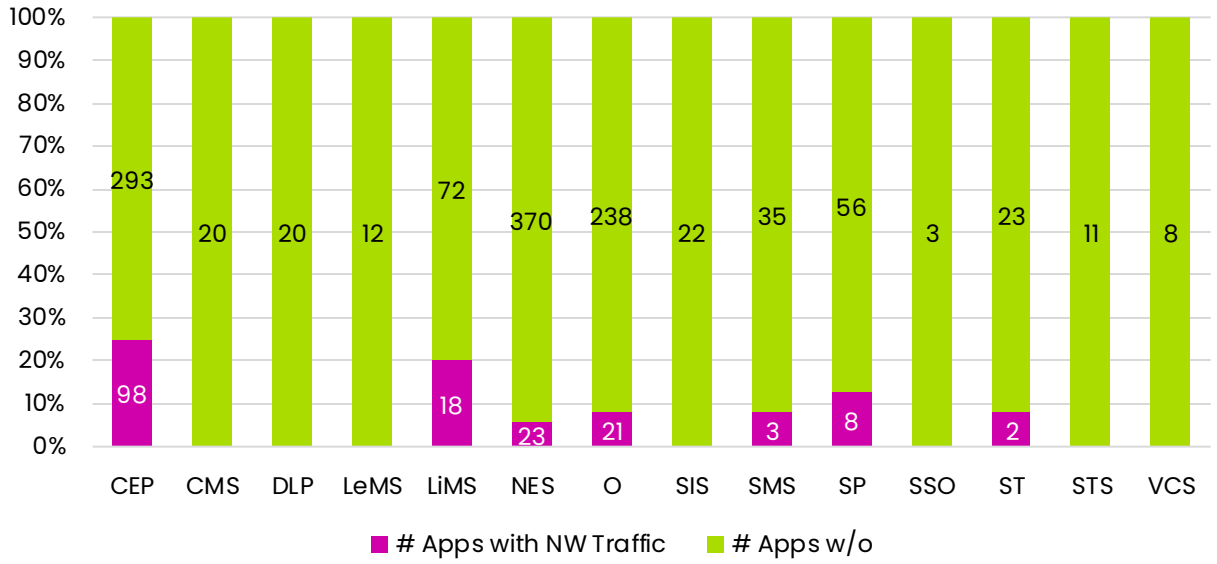


Figure 5.108 — # Apps with NW Traffic to Twitter by Category



5.6.6 Platform Data Sharing by OS

- iOS apps more frequently send data to all six large platforms as compared to Android apps. The existence of a discrepancy suggests that future research should look into how development practices differ across platforms.

Figure 5.109 — Apps with NW Traffic to Adobe by OS

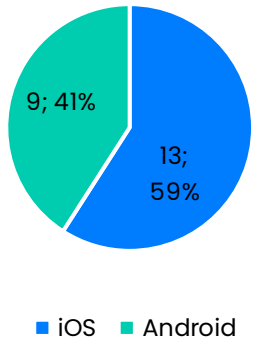


Figure 5.110 — Apps with NW Traffic to Amazon by OS

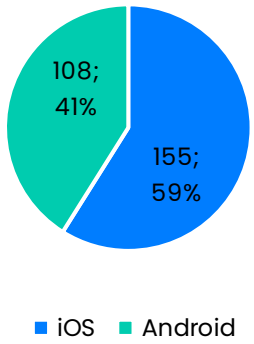


Figure 5.111 — Apps with NW Traffic to Apple by OS

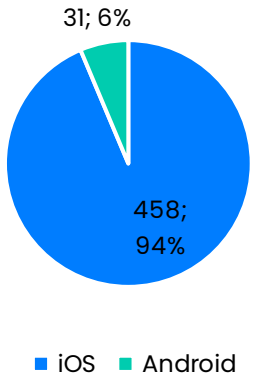


Figure 5.112 — Apps with NW Traffic to Facebook by OS

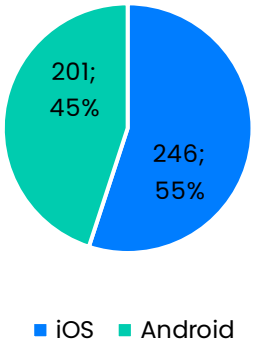


Figure 5.113 — Apps with NW Traffic to Google by OS

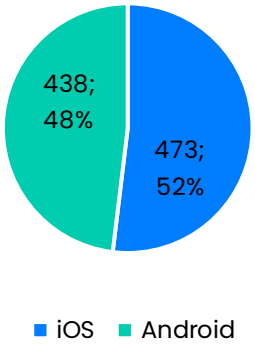
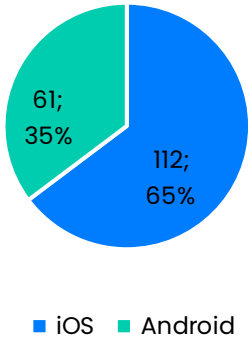
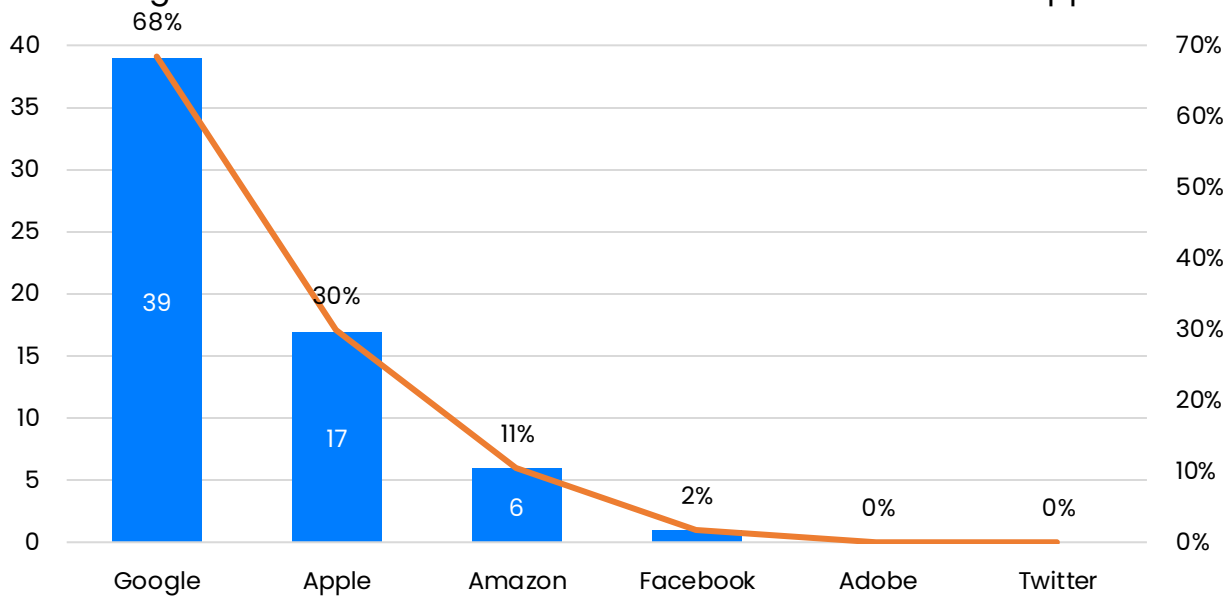


Figure 5.114 — Apps with NW Traffic to Twitter by OS



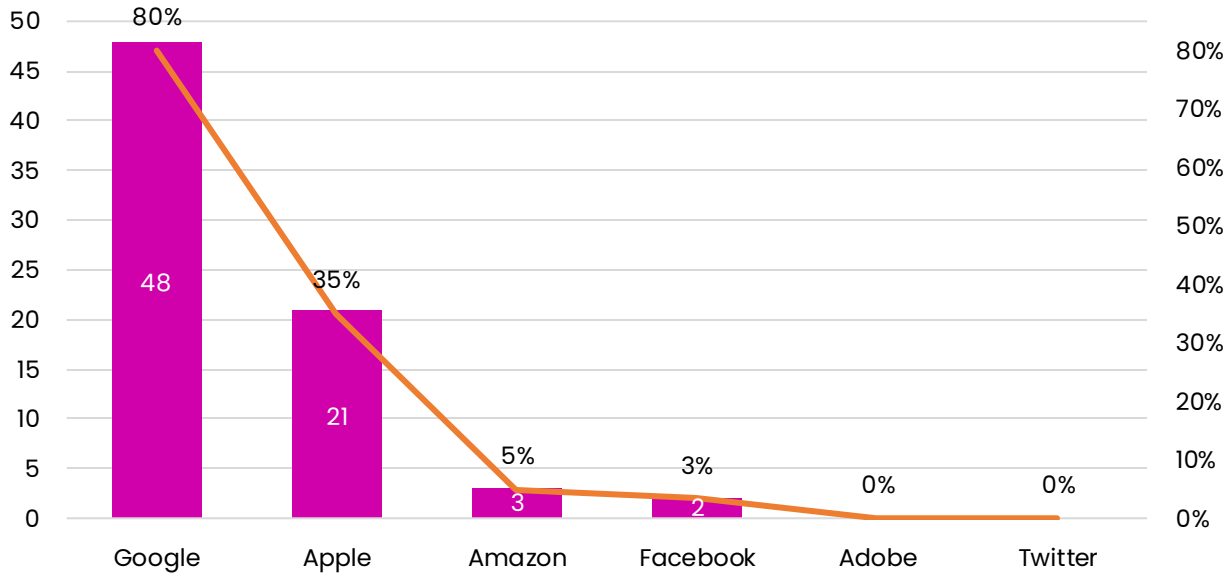
5.6.7 Platform Data Sharing – Most Recommended Apps

Figure 5.115 — Platform Traffic of 25 Most Recommended Apps



5.6.8 Platform Data Sharing – Most Frequently Required Apps

Figure 5.116 — Platform Traffic of Top 25 Mandatory/Key Apps



5.7 25 Safest Apps

We experimented with several different rating schemas to identify the safest and least safe apps. The one we felt provided the most accurate results was based on both the SDKs in the app and the ISL safety score.

To determine most and least safe apps, apps were evaluated in two parts: (1) SDK Composite Scores, and (2) ISL safety score. For 1516 apps, a composite SDK score was determined. This score was calculated as follows:

> SDK Composite Score = [(# of Very High Risk SDKs) + (# of High Risk SDKs / 2) + (# of Medium Risk SDKs / 4) + (# of Neutral Risk SDKs / 8)]

The apps were then sorted by SDK Composite Score.

Least Safe: To qualify as "Least Safe", the apps had to have the highest possible SDK Composite Score AND an ISL safety score of "Do Not Use".

Safest: To qualify as "Safest", the apps had to have the lowest possible score AND an ISL rating of "Some Risk", our best score.

5.7.1 Safest Apps Key Findings

- **100%** of the safest apps were **Generic** apps**,** and most of the apps were **O (46%), NES (25%),** and the remainder were split between SP, LiMS and CMS apps.
    - There is a fairly diverse range of categories, with representation from three core edtech categories.
- **60%** of the safest apps were **Android** apps**.**
- Note that **no CEP** apps were in the top 25 safest apps.

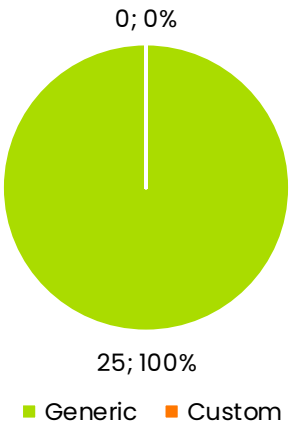
Table 5.5 25 Safest Apps

App Name	Platform	Category	Developer
Manybooks	iOS	NES	Advertical Media LLC
Safe Puzzle	Android	O	Allen Dikio
Capstone Interactive	iOS	O	Capstone Global Ltd.
Virtual Hope Box	iOS	NES	Defence Health Agency and US DoD
DuckDuckGo Privacy Browser	iOS	O	DuckDuckGo
LibAnywhere	Android	LiMS	LibraryThing
Sparky's Firehouse	iOS	O	National Fire Protection Association
Sparky's Fun House	iOS	O	National Fire Protection Association
Sparky's Firehouse	Android	O	National Fire Protection Association
Sparky's Fun House	Android	O	National Fire Protection Association

Safe2Tell CO	iOS	SP	Navigate 360, LLC
P3 Tips	Android	SP	Navigate 360, LLC
Stellarium Mobile - Star Map	Android	O	Noctua Software Ltd.
Rainy Mood Lite	Android	NES	Plain Theory, Inc.
phyphox	Android	O	RWTH Aachen University
Safe Schools Helpline	Android	SP	Security Voice Inc.
Caustic 3	Android	NES	SingleCellSoftware
SaferMT	iOS	SP	Sprigeo
Lexington Public Library	Android	LiMS	The Library Corporation
CareerInfo	iOS	NES	U.S. Department of Labor
CareerInfo	Android	NES	U.S. Department of Labor
Yearbook Snap	iOS	CMS	Walsworth Publishing Company, Inc.
Yearbook Snap	Android	CMS	Walsworth Publishing Company, Inc.
Zoo-phonics 1. The Address Boo	Android	O	Zoo-phonics
Zoo-phonics 2. The Zoo-phonics	Android	O	Zoo-phonics

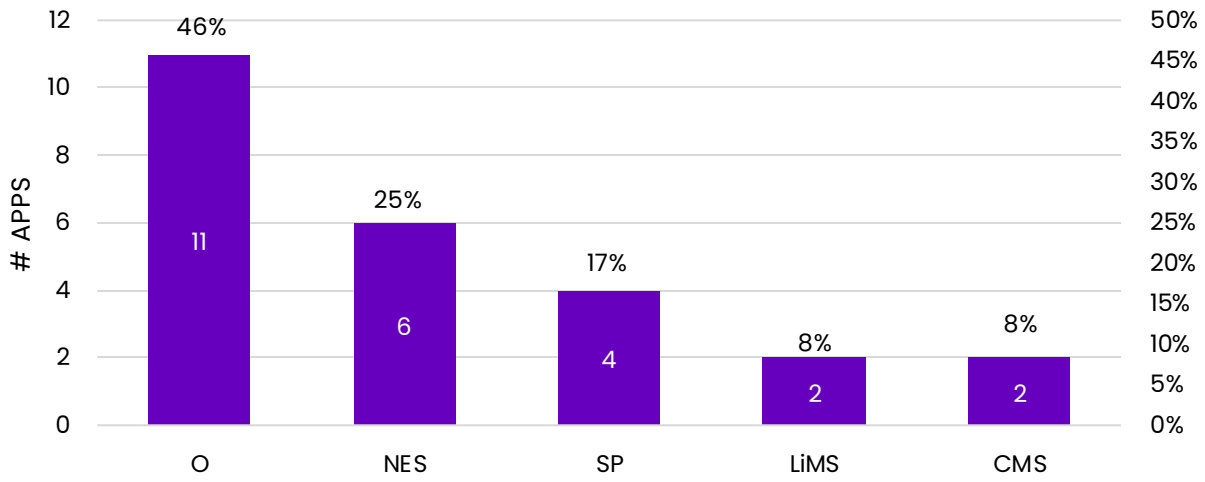
5.7.2 24 Safest Apps by Custom vs. Generic

Figure 5.117 — 25 Safest Apps - Generic vs. Custom



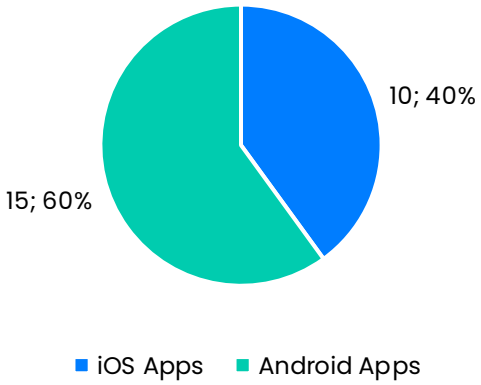
5.7.3 25 Safest Apps by Category

Figure 5.118 — 25 Safest Apps by Category



5.7.4 25 Safest Apps by OS

Figure 5.119 — 24 Safest Apps by OS



5.8 25 Least Safe Apps

5.8.1 25 Least Safe Apps Key Findings

- **88%** of the least safe apps were **Generic**.
- The least safe apps were **NES (68%), O(20%), and CEP (12%).**
- **80%** of the least safe apps were **Android** apps.

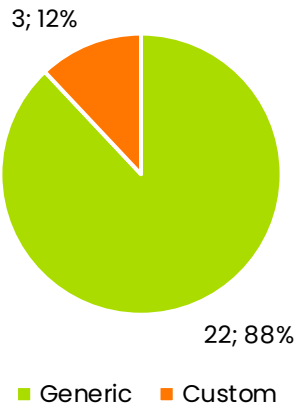
Table 5.6 25 Least Safe Apps

App Name	Platform	Category	Developer
Wattpad - Read & Write Stories	Google	NES	Wattpad Corp.
Happy Color® – Color by Number	Google	NES	X-FLOW LTD
Colorfy: Art Coloring Game	iOS	O	Wildlife Studios
Wordle!	Google	O	Lion Studios, LLC
Flight Pilot: 3D Simulator	Google	NES	Fun Games for Free
Wattpad - Read & Write Stories	iOS	NES	Wattpad Corp.
USA TODAY	Google	NES	Gannett Co., Inc.
Jamestown Sun E-paper	Google	NES	Forum Communications Company
FlipaClip: Create 2D Animation	iOS	NES	Visual Blasters, LLC
CNN Breaking US & World News	Google	NES	Warner Media Companies
Recolor - Adult Coloring Book	Google	NES	Kuuhubb Oy
Flight Pilot Simulator 3D!	iOS	NES	Fun Games for Free
The Wall Street Journal: Busin	Google	NES	Dow Jones & Company, Inc.
FlipaClip: Create 2D Animation	Google	NES	Visual Blasters, LLC
Vestavia Hills Athletics	Google	CEP	SIDEARM Sports, a Learfield Company
Likewise: Entertainment Picks	Google	O	Lightbot
Colorfy: Coloring Book Games	Google	O	Wildlife Studios
Key Ring: Your mobile wallet	Google	NES	InMarket Media LLC
Recolor - Adult Coloring Book	iOS	NES	Kuuhubb Oy
The New York Times	Google	NES	The New York Times Company
Titans Athletics	Google	CEP	From Now On, LLC
Westside Warriors	Google	CEP	From Now On, LLC
AP News	Google	NES	The Associated Press

Sober Grid - Social Network	Google	NES	Sober Grid, Inc
Babbel - Learn Languages	Google	O	Babbel GmbH

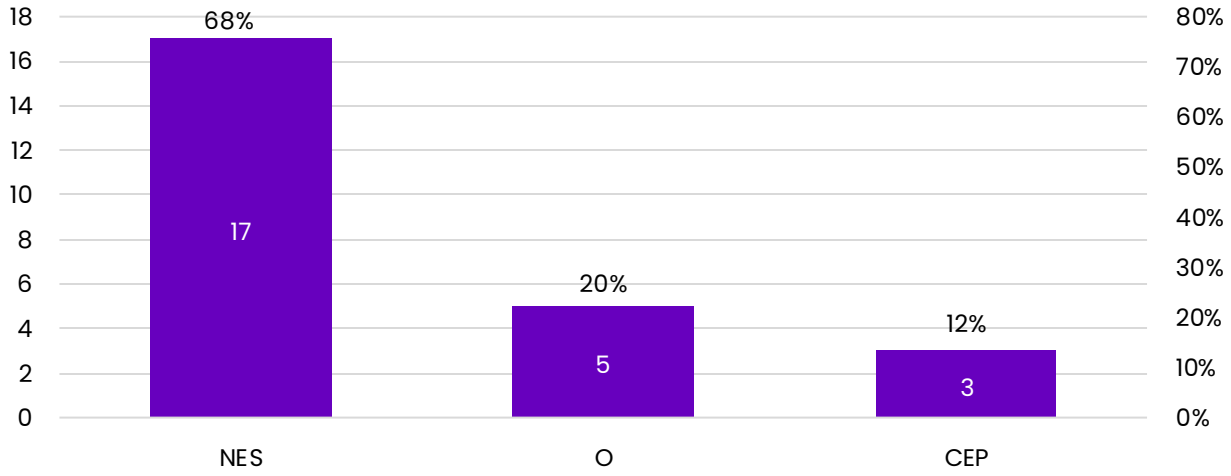
5.8.2 25 Least Safe Apps by Custom vs. Generic

Figure 5.120 — 25 Least Safe Apps - Generic vs. Custom



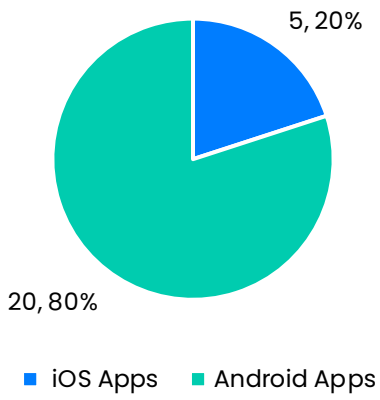
5.8.3 25 Least Safe Apps by Category

Figure 5.121 — 25 Least Safe Apps by Category



5.8.4 25 Least Safe Apps by OS

Figure 5.122 — 25 Least Safe Apps by OS



6 ISL Recommendations

6.1 Schools and Local Educational Agencies

- Schools and LEAs need substantial additional support to better navigate the increasingly complicated and unsafe edtech.
    - Combined with the increasing cybersecurity attacks on LEAs, more financial support and resources are needed.
- Schools should be aware that app publishers are behaving in an unsafe manner and exercise caution about adopting new technologies.
    - When it comes to technologies, until edtech has a safety culture, less is more.

6.2 Edtech Developers

- We see no evidence that edtech developers prioritize safety. The industry needs to join the conversation on software product safety for students.
- Custom, CES type apps must be made safer for students. Being both mandatory and commissioned directly by schools, these should be among the safest apps for students, but that isn't the case.
    - The good news is that a handful of key developers provide most of these apps to schools across the US. They should be able to readily make the necessary safety improvements.
- Advertising must be removed from all edtech apps recommended or required by public schools in the US.
- For developers of edtech who also own advertising related technologies, we suggest that they be required to use a unique domain for the two types of products.
    - For instance, Google should create a new domain, like "googlekids.com", expressly for use in their products that will be used by K12 students.

7 Research Methodology

This research focuses on all technology used by K12 schools included in the sample. This benchmark covers public and private schools across all 50 states in the United States, and the District of Columbia. This study covered 1722 apps in use by the sampled 663 schools, covering a total population of approximately 455,882 students. Schools typically have both Android and Apple iOS version of an app, and both versions were analyzed when available.

7.1 School Selection Methodology

7.1.1 Sampling Procedure

To observe K12 Edtech app usage, 663 total school websites were reviewed by researchers. This sample size was chosen through a power analysis accepting 5% type 1 error and 1.5% margin of error. This suggests a sample size of 680, but in the interest of balanced representation across grades, we settled on 663. In selecting these schools, we made the following four design choices:

A. Representative and balanced sampling across the 50 states.
B. Representative and balanced sampling within the following school types: elementary school, middle school, high school.
C. Sample schools proportionally to the locale distribution of schools in the corresponding state.
D. Only sample schools with over 200 students. Note that we chose this threshold in order to maximize the impact of this benchmark, but this threshold may reduce the number of rural schools sampled.

To satisfy points A and D, we stratified our sample by the 50 states to account for possible differences in technology usage across the 50 states. To ensure balanced representation, we filtered schools with less than 200 students and then sampled 13 schools within each state. For these 13 schools, we decided to sample 12 public schools and 1 private school, 8% of our sample size, approximating the actual private school enrollment of about 9% of all students in the US[5] . Due to lack of technology use disclosure on private schools' websites, we chose to not strive for representation within our sample of private schools as our results would be biased and likely incorrect. Therefore, the next two steps only apply to public schools.

To satisfy point B, these 50 subpopulations (stratum) were then stratified by school type to account for differences in technology usage across grade levels.

[5] https://nces.ed.gov/programs/projections/projections2021/tables/table_01.asp

Again, to ensure balanced representation for public schools we sampled 4 schools of each type.

To satisfy point C, we chose to perform a weighted random sample within each {*state, school type*} subpopulation. These weights were assigned based on the proportion of schools within the corresponding subpopulation that were in each locale. For example, if a subpopulation had 4 schools (2 rural, 1 suburban, 1 urban) a higher weight would be assigned to the rural schools.

In layman terms, we split the population of all schools in the US to 150 sub-populations each corresponding to a particular {*state, school type*} combination. Within each of these 150 sub-populations 4 public schools were sampled where this sampling was weighted to represent the locale distribution of each respective subpopulation.

7.1.2 Sampling Procedure in Practice

Using the above sampling procedure, we used files exported from the National Center for Education Statistics(NCES) to characterize each population and subpopulation. NCES offers csv files containing every school within a particular state. Therefore, we had direct access to the full state subpopulations. Next, to form the school type subpopulations within these state files, each school was assigned to one or more school types based on their grade offerings. Schools were categorized using the following schema:

- Elementary Schools: NCES' *Low-Grade* designation is between PK and 6 and NCES' *High-Grade* designation is between 1 and 6.
- Middle Schools: NCES' *Low-Grade* designation is between PK and 8 and NCES' *High-Grade* designation is between 6 and 8.
- High Schools: NCES' *Low-Grade* designation is between PK and 12 and NCES' *High-Grade* designation is above 8.

This establishes the three subpopulations we want to sample from {*state*, elementary school}, {*state*, middle school} and {*state*, high school}. Next, within each of these subpopulations, we tally up the number of schools within each locale based on the NCES classifications and formulate the sampling weights which define the probability that each school would be selected using our random sample. Finally, the sampling was performed using a weighted random sample computer program forming a representative sample for all schools in the United States with over 200 students.

For example, for New York, we downloaded a dataset containing each school in the state of New York; this dataset is the population of all schools in the New York

subpopulation. Then each school was categorized using the above schema and the weights were formulated.

7.2 App Selection

For each school in the sample, we utilized several methods to determine the technologies and apps in use by the school or school district, including:

- School or school district website manual discovery (looking for "Technology" information, for example).
- Site-search on the school or district website for key terms like "apps".
- Searching AppFigures for the school name or school district name.

Note that we did not contact schools to confirm the technologies found in this way.

7.2.1 Key/Mandatory Apps

Through the app identification process, we observed that some apps were school- or even district-wide deployments, as evidenced by prominent positions on websites. This could be in the form of dedicated login buttons or menu options on the school website, or dedicated training pages or modules [for specific technology]. Note that we did not confirm if the technologies were, in fact, mandatory with the schools.

7.3 Data Collection

In order to answer the research questions described in Section 4.5 we performed two different types of data collection:

- School data collection, and
- App data collection.

7.3.1 School Data Collected

For each school in the sample, we recorded the following information from NCES:

1. # of students
2. School District
3. Geographical Description (Urban / Suburban / Rural)
4. Majority Ethnicity/Race
5. Income Level
6. Public/private
7. Grade levels

To gauge school use of technology, we recorded the following information from school and school district websites:

1. List of apps used by school

a. An indication for each app if it was considered as “mandatory” or “key technology” for the school.

2. Technology Vetting practices
3. Notice and Consent practices for data collection
4. Presence of School-issued devices, and privacy policies for same
5. Number and riskiness of trackers on school website and names of aggregating companies tracking. Specifically, we used EFF’s Privacy Badger and recorded the number and company behind the red and yellow flagged trackers.[6]

> “Red means that content from this third party domain has been completely disallowed.
>
> Yellow means that the third party domain appears to be trying to track you, but it is on Privacy Badger’s cookie-blocking “yellowlist” of third party domains that, when analyzed, seemed to be necessary for Web functionality. In that case, Privacy Badger will load content from the domain but will try to screen out third party cookies and referrers from it.”

6. Platform provider for website
7. Whether there is advertising present on the school website

7.3.2 App Data Collected

For analyzing apps, two primary methods of data collection were used:

- Metadata collection, using information found in the app stores, privacy policy, and in the AppFigures database.
- Observed App Behaviors, from using the app, including capturing network traffic while using the app.

7.3.2.1 App Metadata Collected

ISL utilized tools from AppFigures.com, a mobile app analytics firm which provides a database of software development kits (SDKs), permissions, and other data about mobile apps across all the major app stores. A crucial part of the research methodology was to use AppFigures to study both the number and the type of SDKs included in each app. In addition, we utilized our proprietary ISL SDK Risk Dictionary which provides an ISL Safety Score for every SDK based on its potential for harm.

The following metadata was collected for each app identified as being used by a school in the sample set:

1. App Name

[6] EFF Privacy Badger (https://privacybadger.org/)

2. App Store link
3. App Developer
4. Operating System
5. Custom or Generic app
6. Edtech Category/Classification
7. App Age Level
8. App Release Date
9. App Last Updated Date
10. # downloads (Android only)
11. App Functions
12. SDK list – collected for each app:
    a. Total # of SDKs in the app,
    b. Distribution of SDKs by ISL Safety Score (Neutral Risk, Medium Risk, High-Risk, Very High Risk [Data Broker])
13. Data Accessible by all data controllers and processors as determined by evaluating app permissions.
14. Certifications (e.g. iKeepSafe)
15. Whether or not the iOS privacy label is present (iOS apps only)
16. Privacy Policy URL
    a. Whether the PP has an explicit exclusion for children

7.3.2.2 Observed App Behaviors

ISL used two techniques to measure actual app behaviors:

- Exercising/using the app itself, and
- Observing network traffic to/from the app.

7.3.2.2.1 Data From App Usage

The following information was obtained by using the apps:

1. Whether the app requires login credentials for use
2. Whether unusual/unsafe login behaviors were observed
3. If the app has a "do not sell" [my data] button (California regulation)
4. If the app breaks after a "monster in the middle" attack
5. Whether any dangling domains (unresolved urls) were observed
6. Whether any hijacked domains were observed
7. Whether the app was built using WebView methods
8. Whether advertising is present in the app
9. Whether retargeting ads are present in the app
10. Whether MaxPreps is included in the app (MaxPreps is a problematic school sports service we first identified in this report; the service is ad-funded and still contains retargeting ads)

11. Whether Adobe is present in the UI
12. Whether Amazon in present in the UI

7.3.2.2.2 Network Data Traffic

To measure network traffic, the team utilized Charles Proxy for iOS apps and PCAPdroid for Android apps. These are debugging tools that allow the auditor to capture and view all the HTTP and SSL/HTTPS traffic between the mobile app and external servers.

From this observed network traffic we can derive the list of unique domains, which shows which entities are, in fact, receiving information, and what information is being shared with third parties.

For this phase of reporting, we have distilled the following information directly from the app's network traffic:

1. If Adobe is present in network traffic
2. If Amazon is present in network traffic
3. If Apple is present in network traffic
4. If Facebook is present in network traffic
5. If Google is present in network traffic
6. If Twitter is present in network traffic

More information will be gleaned from ongoing analysis of the network traffic logs.

8 Appendix A: K12 Edtech Typology

The following Edtech classification schemas were considered in deriving our final Edtech typology:

- Valuates Reports': K-12 Education Technology Market Research Report, January 2022, K12 Education Technology Market Size, Share, Growth, Forecast 2021 - 2026 | Valuates Reports
- EdSurge Product Index, Homepage | EdSurge Product Index
- LMS Hero, "What Is Edtech and How Is It Shaping the Future of Learning", What Is Edtech and How Is It Shaping The Future Of Learning - LMS Hero
- "Understanding the Edtech Product Landscape [+Infographic]", Ashmeet Singh, April 19, 2018, https://medium.com/the-edtech-world/edtech-landscape-743716608675
- EdtechImpact.com Categories, https://edtechimpact.com/categories
- Learn Platform, "Edtech Top 40 Mid-Year Report 2021-2022", Edtech Top 40 Mid-Year Report — LearnPlatform
- G2 Edtech Categories, https://www.g2.com/categories/education

After reviewing all the references above, we chose to use the G2 Edtech Categories as the basis for classifying apps in our benchmark, but adding two new categories: Other, for educational-other apps, and NES for Non-Education Specific apps.

Classroom Messaging Software (CMS)

(1) Include multimedia messaging options
(2) Provide mass messaging and push notifications
(3) Facilitate two-way parent-teacher messaging
(4) Sync messages to multiple platforms, including email
(5) Examples: PowerSchool Mobile, School Messenger

Community Engagement Platform (CEP)

(1) Provide tools for administrators and parents to communicate
(2) Include a news feed of recent things happening at the school, for the benefit of both students and parents
(3) Primary function is to serve as a communication platform
(4) Not classified as something else (like SMS)
(5) Examples: Nearpod, Minga

Digital Learning Platform (DLP)

(1) Be designed for use by instructors at K–12 schools or higher education institutions
(2) Deliver interactive educational lessons

(3) Include multimedia elements designed to increase student engagement
(4) Personalize the learning experience for each student
(5) Generate reports based on student performance data (Optional)
(6) Examples: Edmodo, Quizizz

Learning Management System (LeMS)

(1) Provide a platform for educators to deliver online course content to students
(2) Distribute assignments to students and allow instructors to grade student work
(3) Administer digital assessments to students
(4) Facilitate individualized feedback on student work, such as through written comments or grading rubrics
(5) Generate performance dashboards for tracking student progress
(6) Contain gradebook functionality or integrate with third-party gradebooks
(7) Examples: Canvas Student, Google Classroom, Schoology

Library Management Software (LiMS)

(1) Include a database that can be used to store and manage information on different types of content assets (books, magazines, movies, music records, and more) in different formats (print, electronic, video, etc.)
(2) Manage patron and member information including profiles, present and past loans, payments, and penalties
(3) Allow users to find information from public sources like OPAC (Online Public Access Catalog) or WorldCat
(4) Manage asset inventory and loans across multiple physical locations
(5) Provide statistics on loans, inventory, late returns, or lost documents
(6) Examples: Destiny Discover, hoopla, SORA, Libby

Non-Education Specific (NES)

(1) Either not an edtech application or does not fit any categories
(2) Add subcategories of NES
    a. News
        i. Examples: NY Times, KQED
    b. References
        i. Examples: TED talks, Encyclopedia Britannica
    c. Productivity
        i. Examples: Outlook, Google Documents

Other (O)

(1) Edtech/edtech-adjacent applications that do not fit criteria for other edtech categories (e.g. educational games, music lesson apps)
(2) Add subcategory for Games.
    a. Examples: zoo-phonics, Teach Your Monster to Read
(3) Add subcategory for Sports
    a. Examples: ScoreStream, SBLive Sports, NFHS Network

School Transportation Software (STS)

(1) Be designed to manage school transportation programs
(2) Create optimized bus routes and schedules
(3) Assign students and drivers to bus routes
(4) Examples: WheresTheBus, Z Pass+, Versatrans My Stop

Safety Platform (SP)

(1) Allows reporting of school specific safety information to school security personnel
(2) Reporting is anonymous
(3) Examples: WeTip, Vector Alert, P3 Tips

Single Sign On (SSO)

(1) Allows users to use one login to access multiple applications or databases in one portal
(2) Example: Clever, ClassLink LaunchPad

School Management Software (SMS)

(1) Provide tools to improve staff communication
(2) Have features designed to improve efficiency
(3) Include functionality designed to help manage school operations in areas such as facilities, IT management, program management, document management, attendance, food service and payment technologies, hall pass management.
(4) Examples: Nutrislice, MySchoolBucks

Student Information System (SIS)

(1) Monitor relevant student data
(2) Include a portal for parents to access information about their students
(3) Offer reporting capabilities
(4) Handle student admissions
(5) Provides a module for school staff
(6) Examples: OnCourse Connect, Skyward Mobile Access

Study Tools (ST)

(1) Have features specifically for test preparation
(2) Include various study methods
(3) Be accessible for students and educators
(4) Examples: Sporcle, ProProf Quizzes, Kahoot!

Virtual Classroom Software (VCS)

(1) Contain live video streaming capability
(2) Provide screen sharing
(3) Contain an online whiteboard feature
(4) Provide a comprehensive online classroom environment designed for use by educational institutions as well as individual teachers and tutors
(5) Stream live rich media interactive presentations
(6) Examples: Zoom, Microsoft Teams, Google Meet

9 Appendix B: Schools in Sample

ALABAMA
Breitling Elementary School
Fayette County High School
Green Acres Middle School
Haleyville Elementary School
Hartselle Junior High School
Highland Garden Elementary School
Jemison High School
Martin Luther King Jr Elementary School
North Jefferson Middle School
Pell City High School
Sardis Middle School
Trinity Presbyterian School
Vestavia Hills High School
ALASKA
Alaska Middle College School
Anchor Lutheran School
Bettye Davis East Anchorage High School
Central Middle School of Science
Dena'ina Elementary School
Kodiak Middle School
Nome-Beltz Middle/High
Ocean View Elementary
Russian Jack Elementary
Sitka High School
Skyview Middle School
Snowshoe Elementary
Wendler Middle School
ARIZONA
TAPBI (Technology Assisted Project-Based Instruction) //// Now Tempe Union Online
Bogle Junior High School
Sierra Linda High School
Sunnyslope Elementary School
Canyon Springs STEM Academy
High Desert Middle School
Marshall Ranch Elementary School
Pioneer Preparatory - A Challenge Foundation
Sequoia Elementary School
Frances Brandon-Pickett Elementary
Cesar Chavez Elementary
San Miguel High School
Alta Vista High School

ARKANSAS

Bismark Middle School
Chicot Elementary School
Estem Elementary School
Harmony Grove High School
Jacksonville High School
Joe T.Robinson Middle School
Lavaca Middle School
Mayflower Middle School
Northside High School
Reagan Elementary School
Stewart Elementary School
The New School
Westside High School

CALIFORNIA

Beattie Middle
Cesar E. Chavez High
Charles Wright Elementary
Diamond Bar High
Downtown Business High
Hamilton Middle
Hiram W. Johnson High
McKee Middle
Northwood Elementary
Rio Vista Middle
San Benito Elementary
St John Catholic School
Village Elementary Charter

COLORADO

Aurora West College Preparatory Academy
Carmody Middle School
Crown Point Charter Academy
Dolores Secondary School
Iowa Elementary School
Lewis-Palmer Elementary School
Mitchell Elementary School
Most Precious Blood School
Mountain Phoenix Community School
Mountain Vista High School
Sanford Elementary School
Sky View Middle School
Union Colony Preparatory School

CONNECTICUT

Central High School
Fletcher W. Judson School
High School In The Community

Intermediate School
King Philip Middle School
New Fairfield High School
Norte Dame Catholic High School
Pond Hill School
Putnam Middle School
Reed Intermediate School
Thompson Middle School
Tolland Intermediate School
Waterford High School

DELAWARE

Bedford (Gunning) Middle School
Clayton Intermediate School
Dickinson (John) School
duPont (Alexis I.) High School
Fred Fifer III Middle School
Glasgow High School
John Bassett Moore Intermediate School
Lorewood Grove Elementary School
Nellie Hughes Stokes Elementary School
Ross (Lulu M.) Elementary School
Smyrna High School
St May Magdalen School
Talley Middle School

DISTRICT OF COLUMBIA

Anacostia HS
Bridges PCS
Charles Hart MS
Dunbar HS
Eastern HS
Friendship PCS - Collegiate Academy
Kelly Miller MS
Randle Highlands ES
School-Within-School at Goding
ST Peter School
Turner ES
Washington Global Pcs
Washington Latin PCS - MS

FLORIDA

Abess Park Elementary School
Avant School of Excellence
Beacon Cove Intermediate School
Braden River High School
Homestead Middle School
Lake George Elementary
Lake Nona High School

Lake Wales Senior High School
Plant City High School
Rockway Middle School
Tradewinds Middle School
Wakulla Middle School
Williston Elementary School

GEORGIA

Alto Park Elementary School
Bonaire Middle School
Central High School
Central Middle School
East Hall High School
East Laurens Middle School
G.W. Carver High School Early College
New Creation Christian Academy
Richmond Hill Middle School
Smith-Barnes Elementary School
Spalding High School
Woodlawn Elementary School
Worth County Elementary School

HAWAII

Ewa Makai Middle School
Henry Perrine Baldwin High School
Hokulani Elementary School
King Kekaulike High School
Major General William R Shafter Elementary School
Maui Waena Intermediate School
Mililani Uka Elementary School
Sacred Hearts School & Early Learning Center
Waiakea Intermediate School
Waianae Elementary School
Waimea Canyon Middle School
Waipahu High School
West Hawaii Explorations Academy

IDAHO

East Valley Middle School
Joplin Elementary School
Marsh Valley High School
Nampa Christian Schools
Renaissance High School
Sawtooth Elementary School
Shadow Hills Elementary
Skyview High School
St. Maries Middle School

Taylorview Middle School
Timberline High School
Van Buren Elementary School
Village Leadership Academy

ILLINOIS

Ascension Elementary School
Brooks College Prep Academy HS
Everett F Kerr Middle School
Golf Middle School
Gompers Junior High School
Hinsdale South High School
Lake Forest High School
Lincoln Elem School
Lyon Magnet Elementary School
Pittsfield High School
Pleasant Ridge Elem School
Tonti Elem School
Washington Middle School

INDIANA

Avon Intermediate School East
Bittersweet Elementary School
Central Catholic
East Noble Middle School
Hamilton SE Int and Jr High Sch
Michael Grimmer Middle School
Northeast Dubois Jr/Sr High School
Prince Chapman Academy
Rising Sun High School
Scottsburg Senior High School
Stonegate Elementary
Tipton High School
Zionsville Middle School

IOWA

Camanche Elementary
Carlisle Middle School
Hoover Middle School
Indianola High School
Jordan Creek Elementary School
Manson Northwest Webster Elementary
MOC-Floyd Valley High School
Morning Star Academy
PCM Middle School
Storm Lake Middle School
Timber Ridge Elementary
West High School
West High School

KANSAS
Blessed Sacrament Catholic School
Burlington Elementary School
Cleaveland Traditional Magnet Elementary
Dodge City High School
Dwight D. Eisenhower Middle School
Hesston Middle
Jefferson West High
North High
Pioneer Trail Middle School
Richard Warren Intermediate School
Roosevelt Elem
Stilwell Elementary
Wamego High
KENTUCKY
Buckhorn School
Crums Lane Elementary
Garrard Middle School
Johnson Central High School
Lafayette High School
Ockerman Elementary School
Owensboro Innovation Middle School
Red Oak Elementary
South Marshall Middle
St. Francis School (Now Francis Parker School)
Summit View Academy
Symsonia Elementary School
Walton-Verona High School
LOUISIANA
Arcadian Middle School
Bayou Blue Middle School
D.C. Reeves Elementary School
Good Hope Middle School
Grayson Elementary School
Loranger Middle School
Meaux Elementary School
New Orleans Center for Creative Arts
Northeast High School
Parkway High School
St Peter Chanel Interparochial School
Tanglewood Elementary School
Woodlawn High School
MAINE
Biddeford Middle School
C K Burns School

Ellsworth High School
Eva Hoyt Zippel School
Frank H Harrison Middle School
Manchester School
Maranacook Community High Sch
Oak Hill Middle School
Orono High School
Skowhegan Area Middle School
Thornton Academy
Vickery School
Wells High School

MARYLAND

Bayside Elementary School
Benjamin Stoddert Middle School
Carver Vocational-Technical High
Cherokee Lane Elementary
Chevy Chase Elementary
Ellicott Mills Middle
Lillie May Carroll Jackson School
Martin Luther King Jr. Middle
Maurice J. McDonough High School
Milbrook Elementary
Montgomery Blair High
Oakdale High
Rockbridge Academy

MASSACHUSETTS

Belchertown High
Brookwood School
Elmwood
Gates Middle School
Henri A. Yelle
O'Bryant School Math/Science
Tracy
Turkey Hill Elementary School
Upper Cape Cod Regional Vocational
Technical
Vassal Lane Middle School
Weston Middle School
William R. Peck School
Winthrop High School

MICHIGAN

Benton Harbor High School
Boyd W Arthurs Middle School
Boyne City Middle School
Carl T Renton Jr High School
Detroit Cristo Rey High School

Garber High School
Gladstone Area Middle School
Leslie High School
Onaway Elementary School
Seminole Academy
Troy High School
William A Pearson Elementary
Winchell Elementary School

MINNESOTA

Anderson Elementary
Crossroads Montessori
Deer River Secondary
Joseph Nicollet Middle School
Lakeview Secondary
Minnehaha Academy - Upper School
Monticello Senior High
Oakwood Elementary
Pequot Lakes Middle
Pioneer Ridge Middle School
Royalton Middle School
St. Louis Park Senior High
Sun Path Elementary

MISSISSIPPI

Bettye Mae Jack Middle School
Brandon High School
Callaway High School
Charleston High School
Clinton Jr High School
East Tate Elementary School
Edna M Scott Elementary School
Madison Station Elementary School
Mendenhall Junior High School
Oakhurst Intermediate Academy
R.H. Long Booneville Middle School
Resurrection Catholic School - High School Campus
Tishomingo County High School

MISSOURI

Cold Water Elem.
East Elem
Excelsior Springs 40
Holy Cross Academy
Jackson Middle
Little Blue Elementary
Marshall SR. High
Monroe City R-I High

Pleasant View Middle
Poplar Bluff Jr. High
Portageville Elem.
Ritenour Sr. High
Thomas Jefferson Middle

MONTANA

Browning Middle School
Corvallis High School
Dillon Middle School
Emerson School
Fred Moodry Intermediate
Fred W Graff School
Glacier High School
Malta K-5
Poplar High School
Ronan Middle School
Shepherd High School
Trinity Lutheran School
Valley View School

NEBRASKA

Barr Middle School
Crete Middle School
Douglas Co West High School
Eastridge Elementary School
Mc Cook Junior High School
Norris Intermediate School
Norris Middle School
Northwest High School
Paddock Road Elementary School
Secondary Sch At Raymond
SS Peter & Paul Elementary School
Westmoor Elementary School
Winnebago High School

NEVADA

Albert M. Lowry High School
Brookfield School
Cashman James MS
Centennial HS
Cheyenne HS
Democracy Prep at Agassi High
Diskin P A ES
Fertitta Victoria MS
Givens Linda Rankin ES
Keller Duane D MS
MAMIE TOWLES ELEMENTARY
Tate Myrtle ES

Webb Del E MS

NEW HAMPSHIRE

Bedford High School
Center Woods School
Gonic School
Henry J. McLaughlin Jr. Middle School
Hudson Memorial School
James Mastricola Upper Elementary School
Lebanon High School
Merrimack High School
Merrimack Valley Middle School
Nashua High School South
New Boston Central School
Pennichuck Middle School
Saint Christopher Academy

NEW JERSEY

Crossroads North Middle School
Frelinghuysen Middle School
Hawthorne High School
Merritt Memorial
Ocean City High School
Patrick M Villano School
Russell O. Brackman Middle School
South River Middle School
Swimming River School
Timothy Christian School
Wayne Valley High School
West Morris Mendham High School
Woodland School

NEW MEXICO

Albuquerque High
Annunciation Catholic SchoolntarySchool
Artesia Zia Intermediate
Cameo Elementary
Goddard High
Kirtland Middle
Los Lunas Middle
Marshall Middle
Montessori of the Rio Grande
Oñate Elementary
Pojoaque High
Rio Rancho High
Thoreau Elementary

NEW YORK

Arcadia High School
Cambria Heights Academy

Franklin Delano Roosevelt High School
German Internation School New York
Hamburg Middle School
Hudson Falls Primary School
Jefferson Elementary School
JHS 104 Simon Baruch
North Elementary School
Oneonta Middle School
PS 32 Samuel Mills Sprole
Tottenville High School
Turtle Hook Middle School

NORTH CAROLINA

Carter Community Charter
Chestnut Grove Middle School
Christ School
Cumberland Academy 6-12 Virtual School
Edward Best Elementary School
Haw River Elementary
Heritage Middle School
Holly Shelter Middle
North Buncombe Elementary
Onslow Virtual Secondary
Porter Ridge Elementary
Providence Grove High School
West Lincoln High

NORTH DAKOTA

Heritage Middle School
Jamestown Middle School
Lewis and Clark Elementary School
Mandan Middle School
Nativity Elementary School
Oakes High School
Rugby High School
Sunrise Elementary School
Valley Middle School
Wahpeton High School
Washington Elementary School
Washington Elementary School
Watford City High School

OHIO

Benjamin Logan High School
Brookside Intermediate School
Buckeye Local High School
Carlisle Junior High School
Edgewood Primary School
Hudson Middle School

Huron High School
Little Miami Middle School
Maritime Academy of Toledo The
Salt Creek Intermediate School
St. Benedict Catholic School
W.H. Kirk Middle School
Waterloo Elementary School

OKLAHOMA

Cascia hall Preparatory School
Collinsville MS
Dickson HS
Disney ES
Dove Science Academy MS
Moore HS
Morrison ES
Mustang North MS
Newman MS
Oologah-Talala HS
Tecumseh HS
Thomas ES
Verdigris Upper ES

OREGON

Beatrice Morrow Cannady Elementary
Capital Christian School
David Douglas High School
Eagle Point High School
East Elementary School
French Prairie Middle School
Kalmiopsis Elementary
Millicoma School
Mountain View Senior High School
Myers Elementary School
North Valley High School
Talent Middle School
Whitford Middle School

PENNSYLVANIA

Freedom HS
Albert Gallatin South MS
Apollo-Ridge HS
Barkley El Sch
Chichester MS
Mid Valley Secondary Center
Perry Lower Intrmd Sch
Redbank Valley Intrmd Sch
Roberto Clemente Middle School
St Gabriel-Sorrowful Virgin School

Swatara MS
Thomas W Holtzman Jr El Sch
West Allegheny SHS

RHODE ISLAND

Anthony Carnevale Elementary
Dr Jorge Alvarez HS
East Providence High
George Hanaford School
Kent Heights School
Kickemuit Middle School
La Salle Academy
Lincoln Middle School
Lonsdale Elementary
Nathanael Greene Middle
Pilgrim High School
The Compass School
West Warwick High School

SOUTH CAROLINA

Alcorn Middle
Berea High School
Blue Ridge Middle
Dr. Phinnize J. Fisher Middle
Dutch Fork Elementary
East Cooper Montessori Charter
Legion Collegiate Academy
Maryville Elementary
Mead Hall Episcopal School
North Charleston Elementary
Sandel Elementary
T. L. Hanna High
York Prepatory Academy

SOUTH DAKOTA

Brandon Valley Middle School - 02
Chamberlain Jr. High - 02
George McGovern Middle School - 09
Huron High School
Martin Elementary
North Middle School - 35
Red Cloud Indian School
Todd County Elementary - 16
Vermillion High School - 01
West Central High School - 01
Westside Elementary - 03
Winner High School - 01
Woodrow Wilson Elementary - 17

TENNESSEE

Austin East High/Magnet
Bolivar Elementary
Catlettsburg Elementary School
Central High School
Chester County Junior High School
Columbia Academy
East Hickman Intermediate School
East Ridge Middle School
Farragut Intermediate
John F. Kennedy Middle
Lookout Valley Middle / High School
White House Heritage High School
Whittle Springs Middle School

TEXAS

Anna Middle
Collegiate H S
D J Red Simon Middle
Eagle Pass J H
Garden Ridge El
Glenn H S
Greathouse El
Holy Family Catholic School
Houston Academy For International Studies
Iola El
Mansfield H S
Noemi Dominquez El
Ojeda Middle School

UTAH

Bridger School
Davis Connect K-6
Ecker Hill Middle
J E Cosgriff Memorial Catholic School
Jordan Ridge School
Mountain Green Middle
Mountainside School
North Sanpete High
Park City High
Skyline High
Timpanogos Middle School
Timpview High
West Bountiful School

VERMONT

Founders Memorial School
Bennington Elementary School
Brattleboro Union High School
Christ the King School

Essex Middle School
Fairfield Center School
Green Street School
Hartford High School
Lake Region UHSD #24
Main Street Middle School
Middlebury Union Middle School
Orchard School
South Burlington High School

VIRGINIA

Alexandria City High
Annandale High
Cardinal Forest Elementary School
Clifton Middle
Kempsville Middle
King William High
Meriwether Lewis Elementary
Mountain View Elementary School
Staunton River Middle School
Tuckahoe Middle
Twin Springs High School
Westover Christian Academy
Willard Model Elementary

WASHINGTON

Bellevue Christian School
Edmonds Elementary
Friday Harbor High School
James Sales Elementary
Lakeridge Middle School
Lewis & Clark Middle School
McFarland Middle School
Mossyrock Jr./Sr. High School
Ponderosa Elementary
Ridge View Elementary School
Skyview High School
Todd Beamer High School
WyEast Middle School

WEST VIRGINIA

Bridge Street Middle School
Hedgesville High School
Hinton Area Elementary
Kellogg Elementary School
Lincoln High School
Martinsburg High School
Monongah Middle School
Mountain Ridge Middle School

St. Joseph Catholic School
Summersville Middle School
Warm Springs Intermediate School
Weirton Elementary
Winfield High School

WISCONSIN

Altoona Middle
Bloomer High
D C Everest Middle
Galesville-Ettrick-Trempealeau High
Holmen High
Kewaskum Elementary
Luther High School
New Directions Learning Community
Oak Creek West Middle
Sandhill Elementary
Somerset Elementary
Tomahawk Middle
Viroqua High

WYOMING

Cody Middle School
Davis Middle School
Dildine Elementary
Henry A. Coffeen Elementary
Kemmerer Junior Senior High School
Lander Middle School
Meadowlark Elementary
Pinedale High School
Pinedale Middle School
Pioneer Park Elementary
Rawlins High School
St Anthony Tri-Parish Catholic School
Triumph High School

10 Appendix C: App Developers by Category

Figure 10.1 — Top CEP App Developers by # Apps in Sample

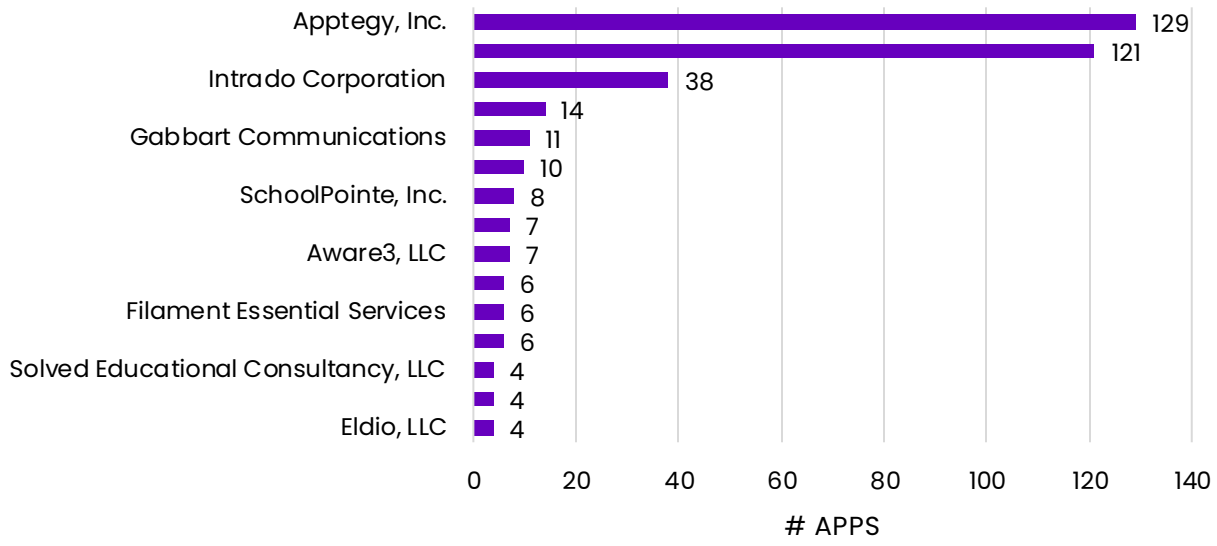


Figure 10.2 — CMS App Developers by # Apps in Sample

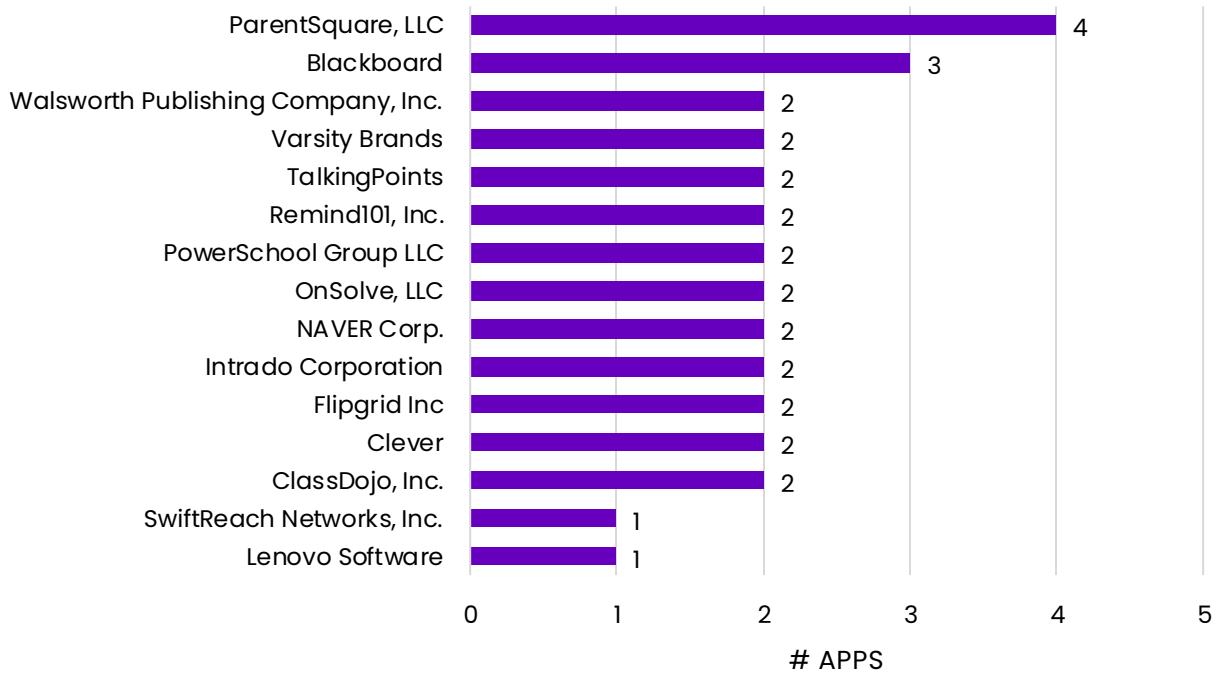


Figure 10.3 — DLP Developers by # Apps in Sample

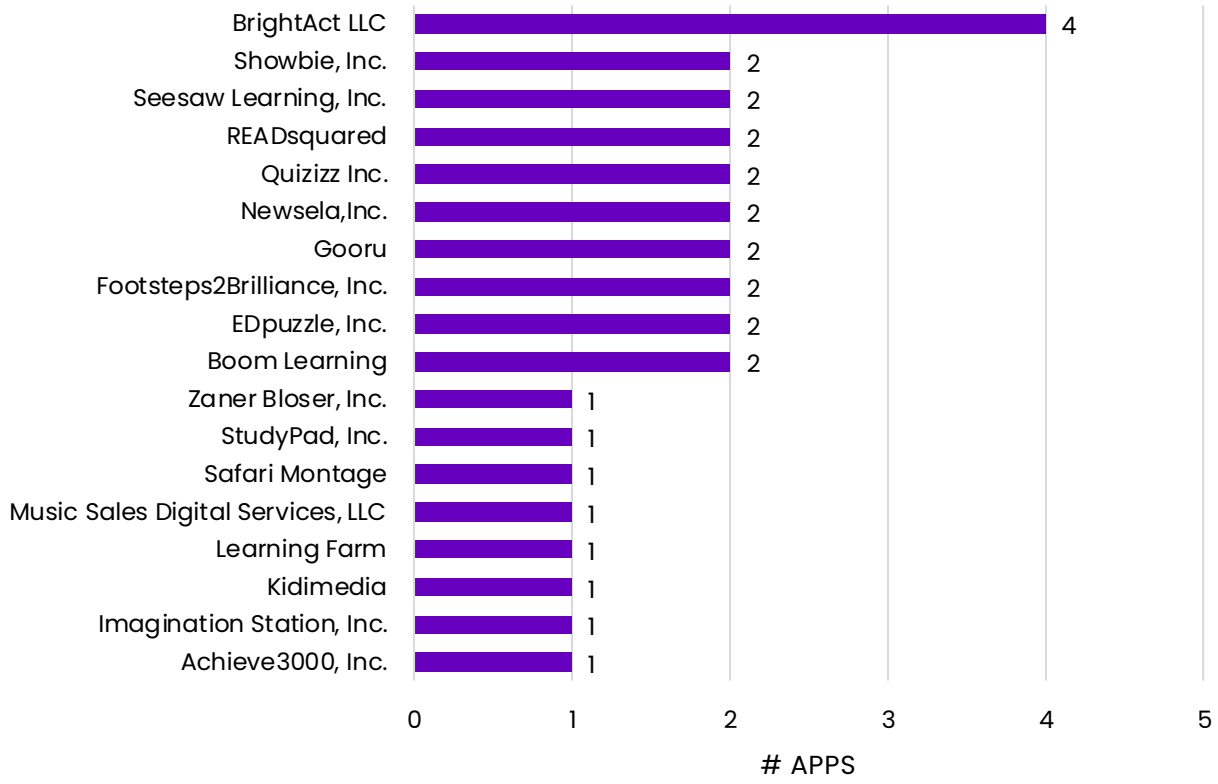


Figure 10.4 — LeMS App Developers by # Apps in Sample

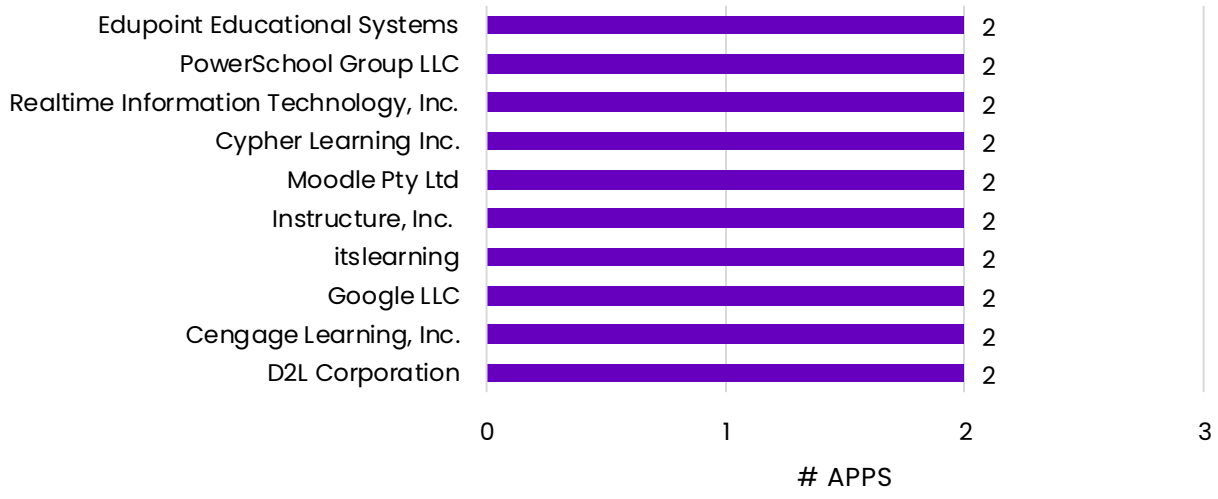


Figure 10.5 — LiMS App Developers by # Apps in Sample

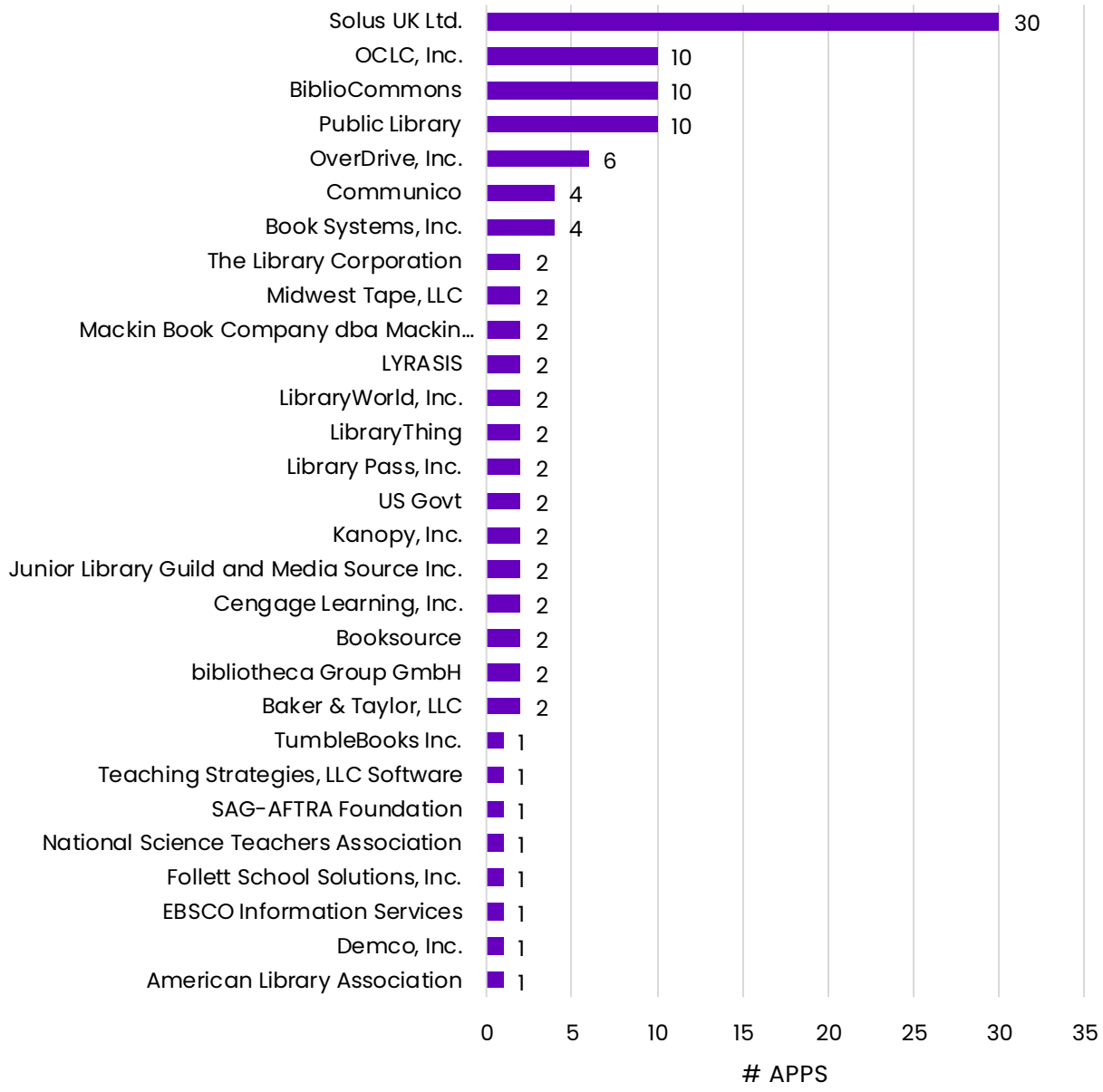


Figure 10.6 — SIS App Developers by # Apps in Sample

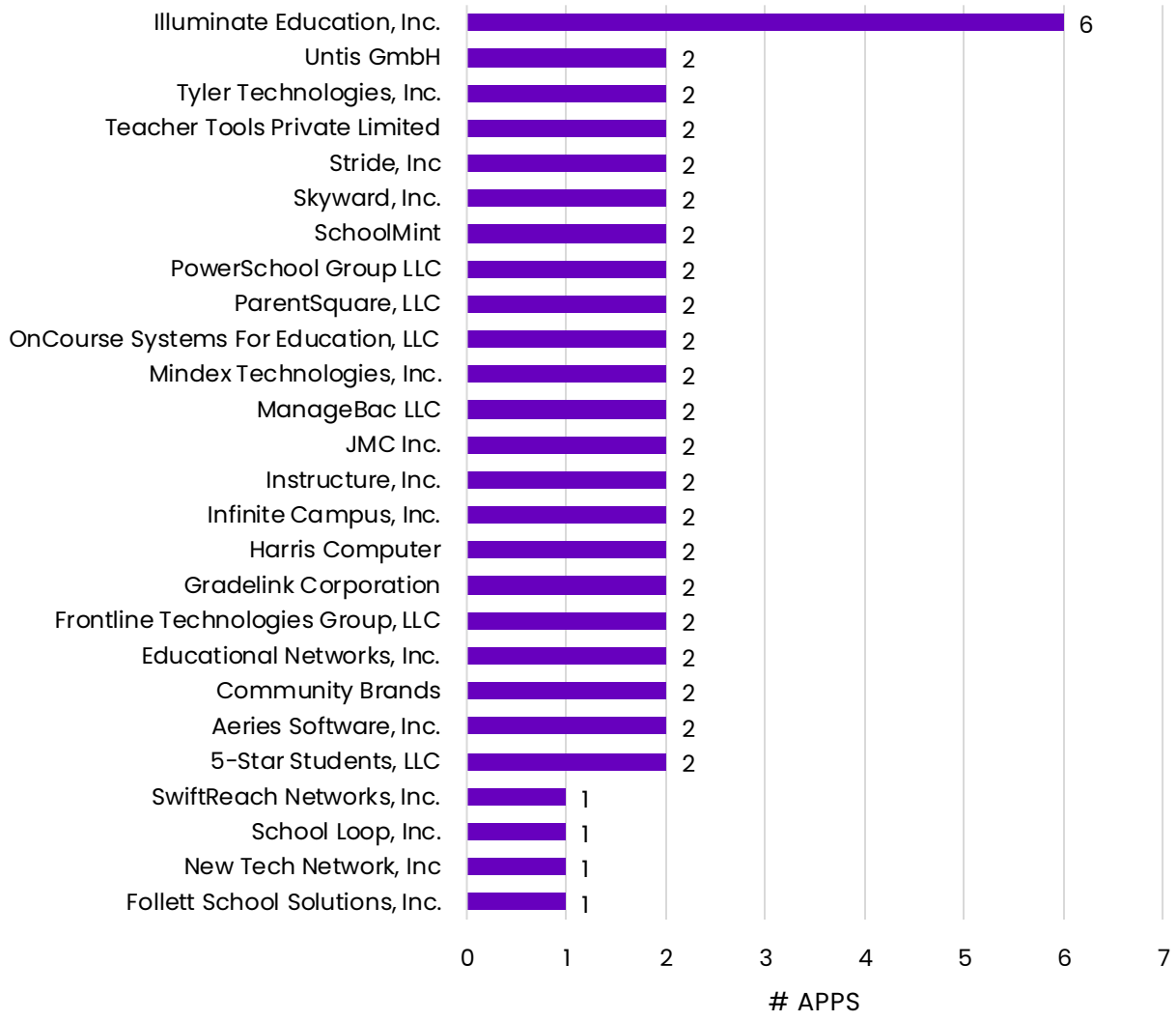


Figure 10.7 — SMS App Developers by # Apps in Sample

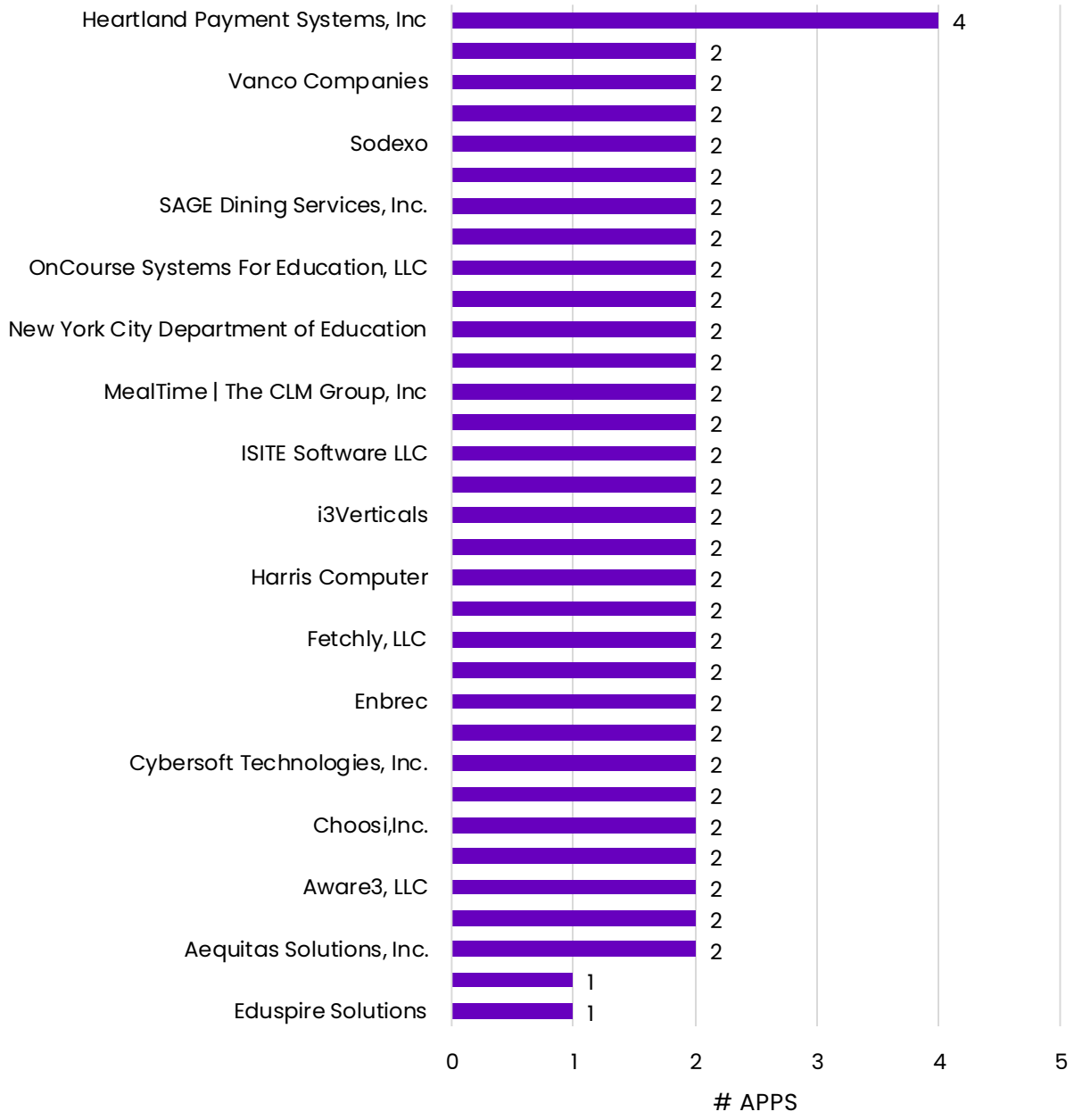


Figure 10.8 — SP App Developers by # of Apps in Sample

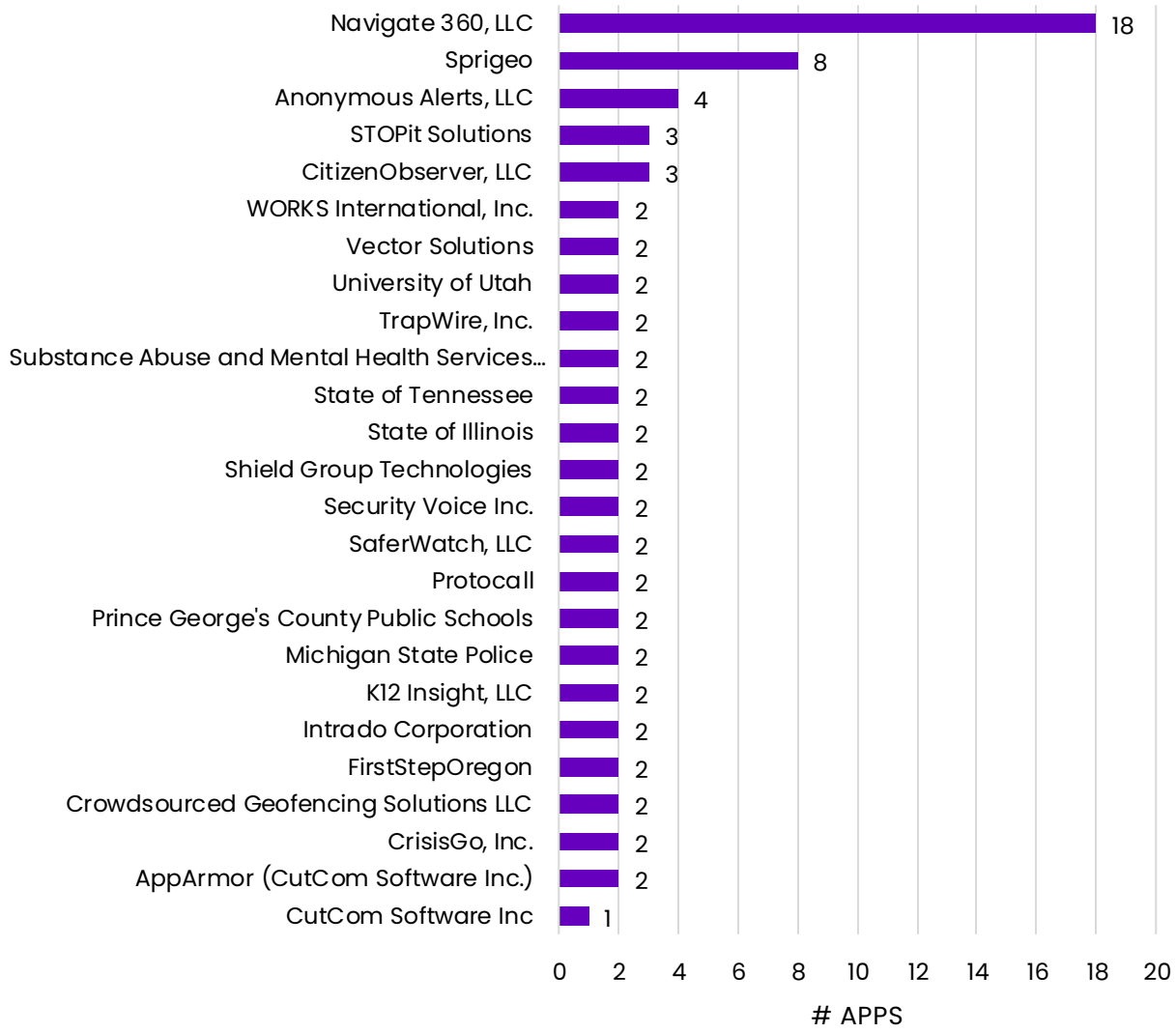


Figure 10.9 — SSO App Developers by # Apps in Sample

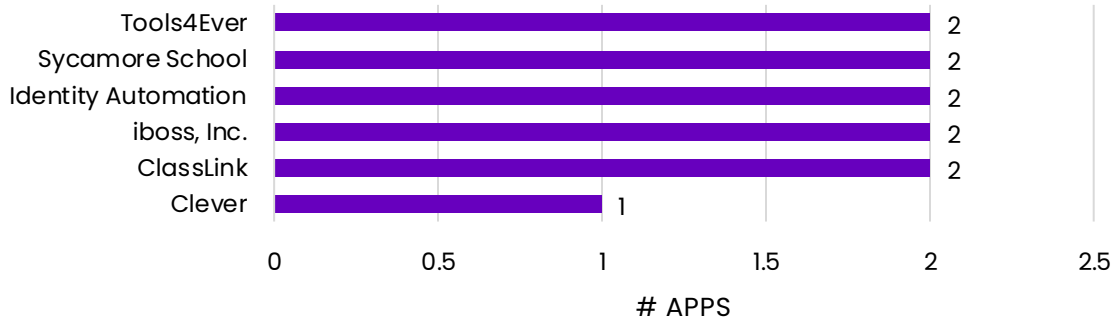


Figure 10.10 — ST App Developers by # Apps in Sample

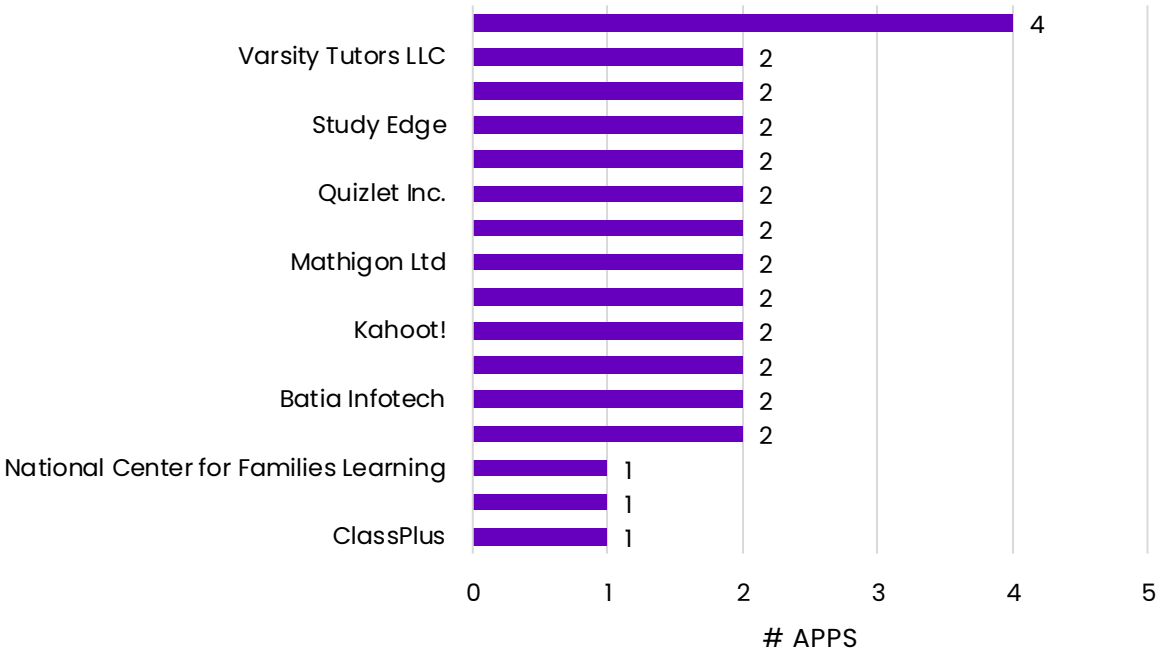


Figure 10.11 — STS App Developers by # Apps in Sample

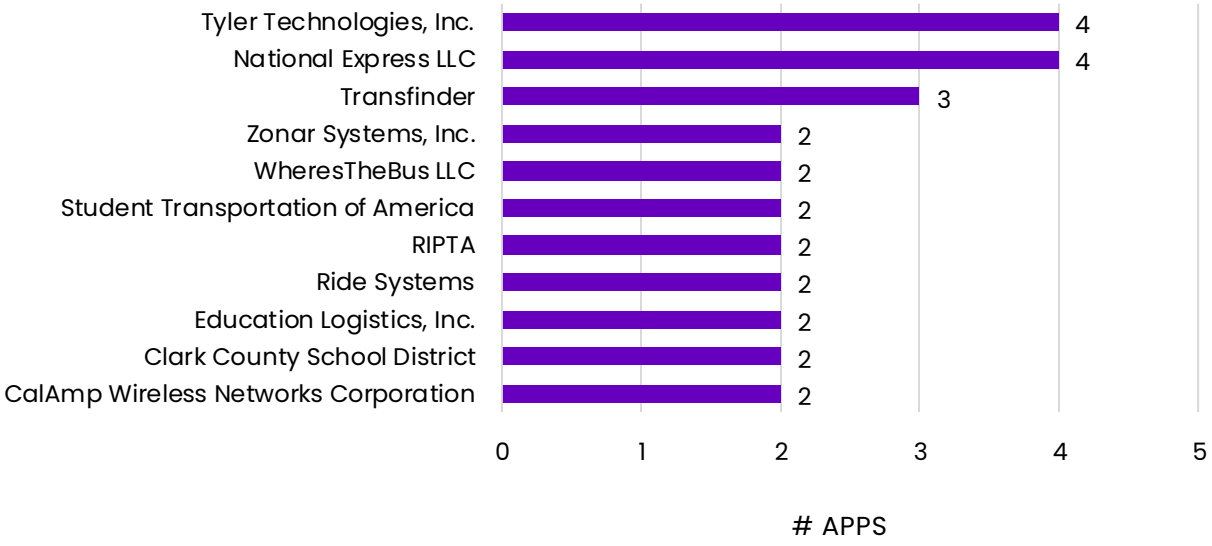
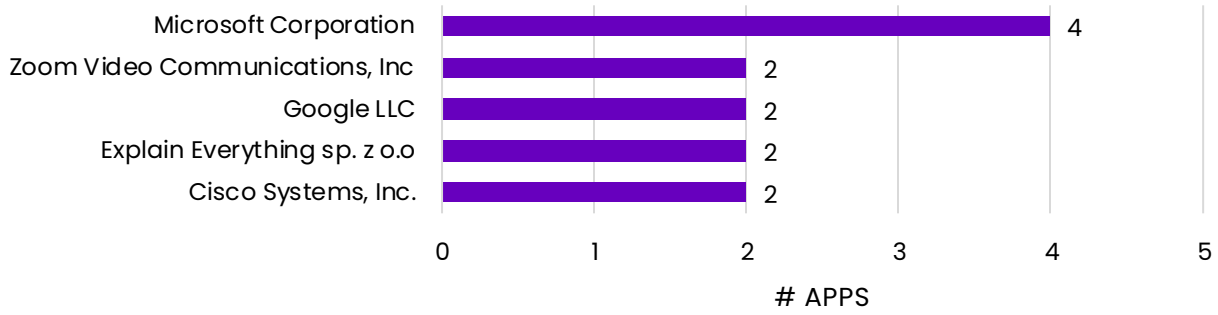


Figure 10.12 — VCS App Developers by # Apps in Sample



11 Appendix D: Permissions by App Category

Figure 11.1 — Permissions - CEP Apps

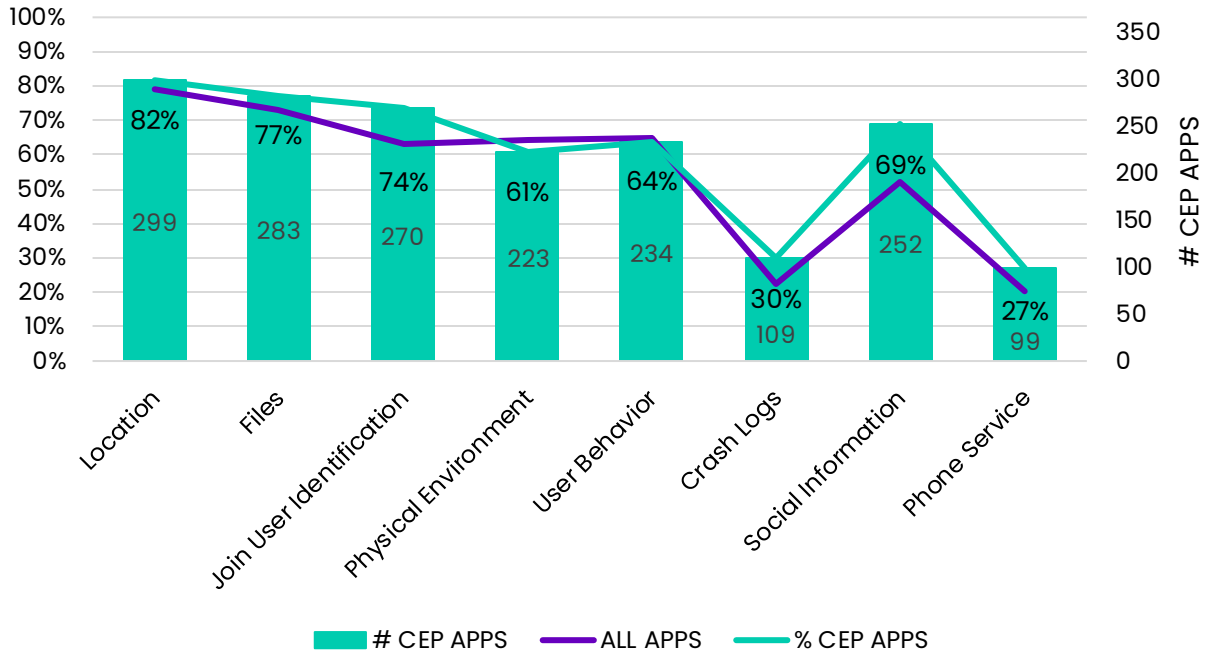


Figure 11.2 — Permissions - CMS Apps

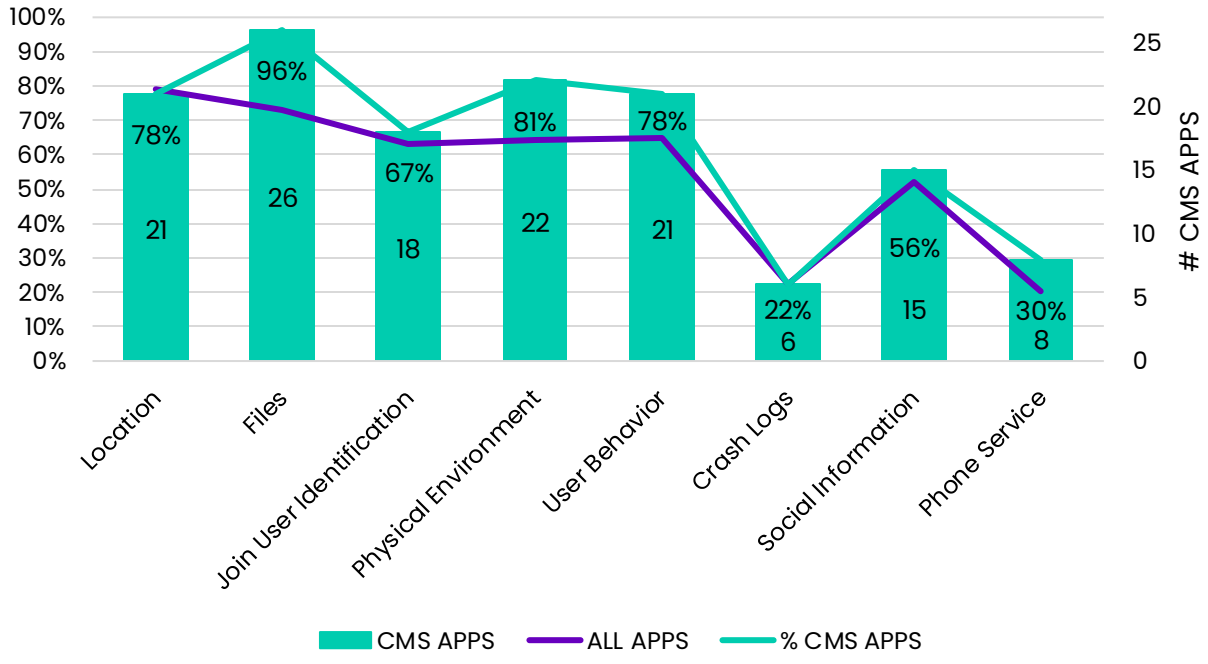


Figure 11.3 — Permissions - DLP Apps

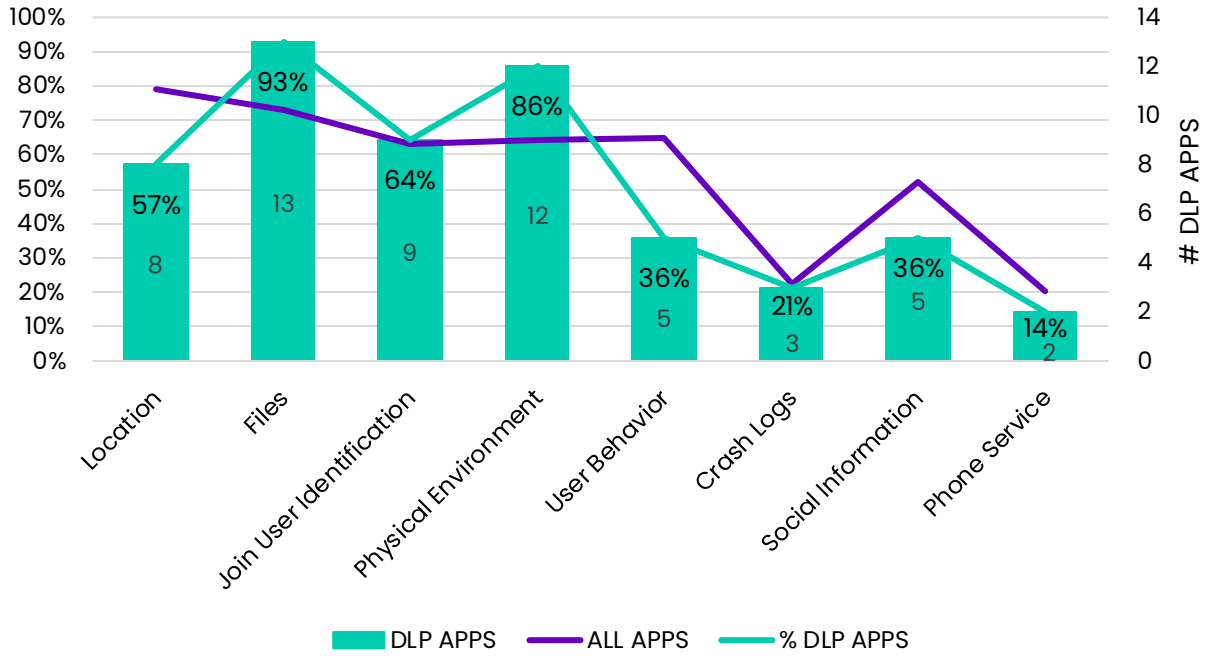


Figure 11.4 — Permissions LeMS Apps

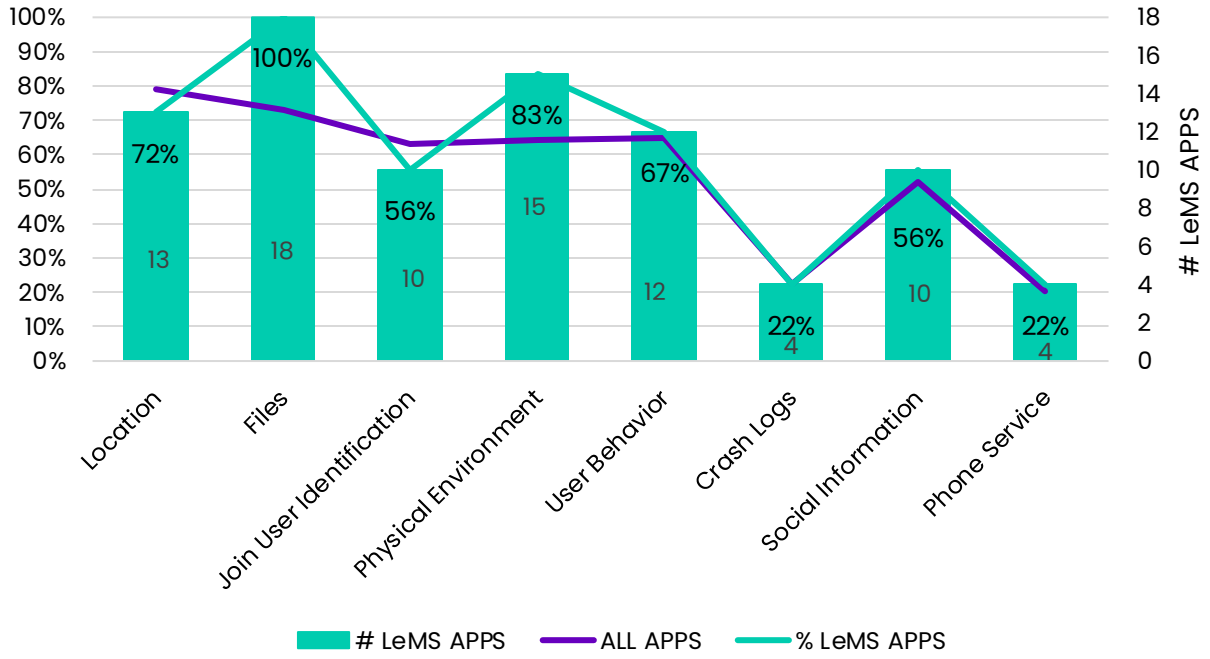


Figure 11.5 — Permissions - LiMS Apps

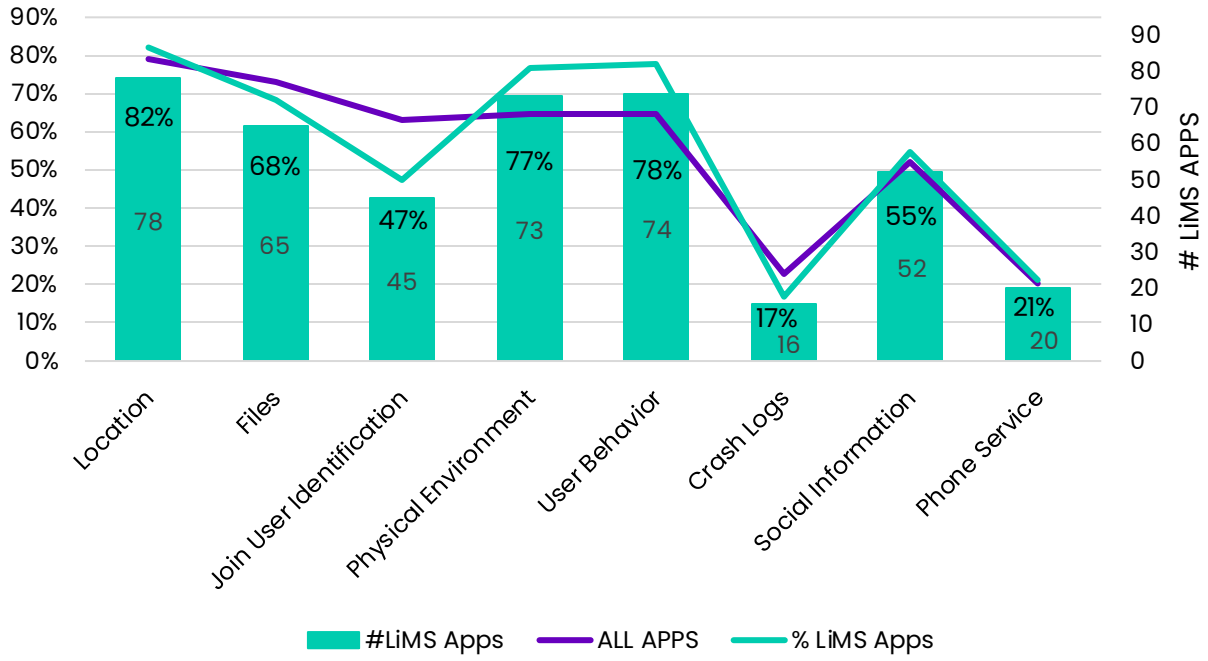


Figure 11.6 — Permissions - NES Apps

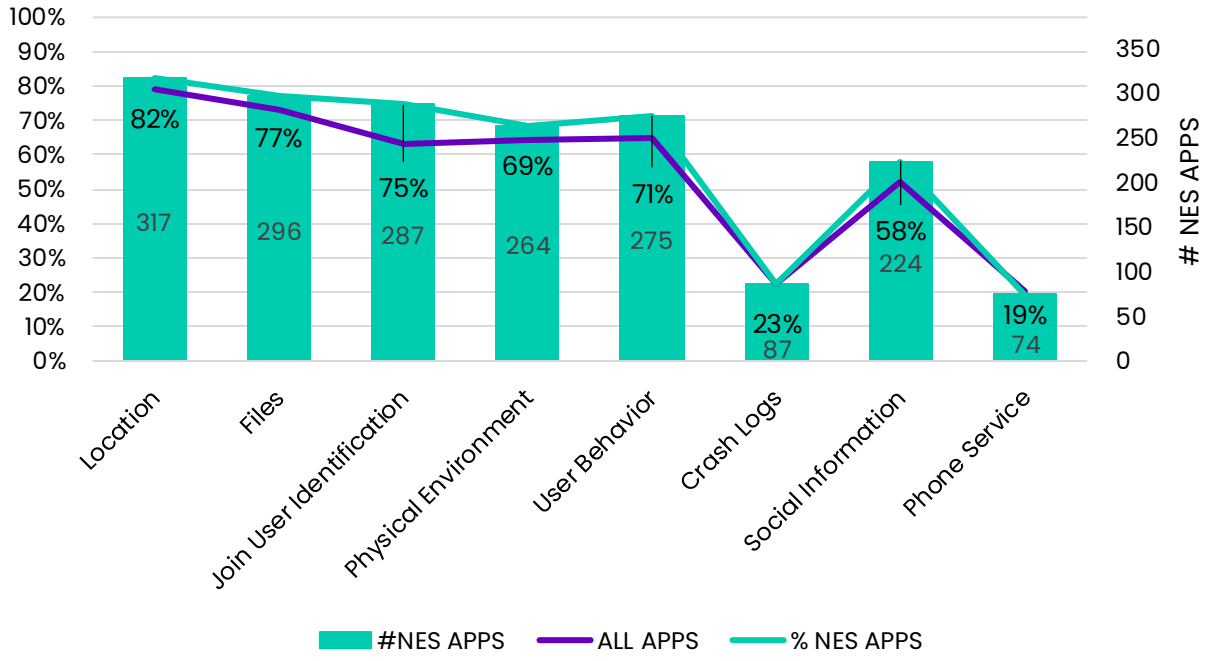


Figure 11.7 — Permissions - O Apps

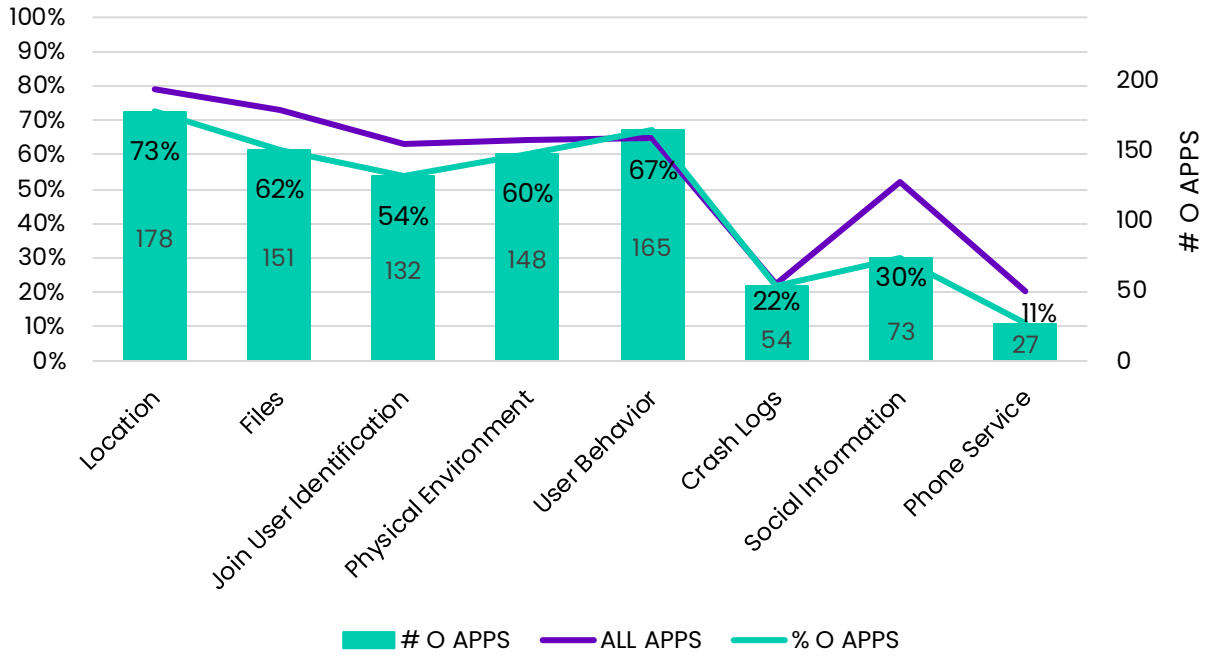


Figure 11.8 — Permissions - SIS Apps

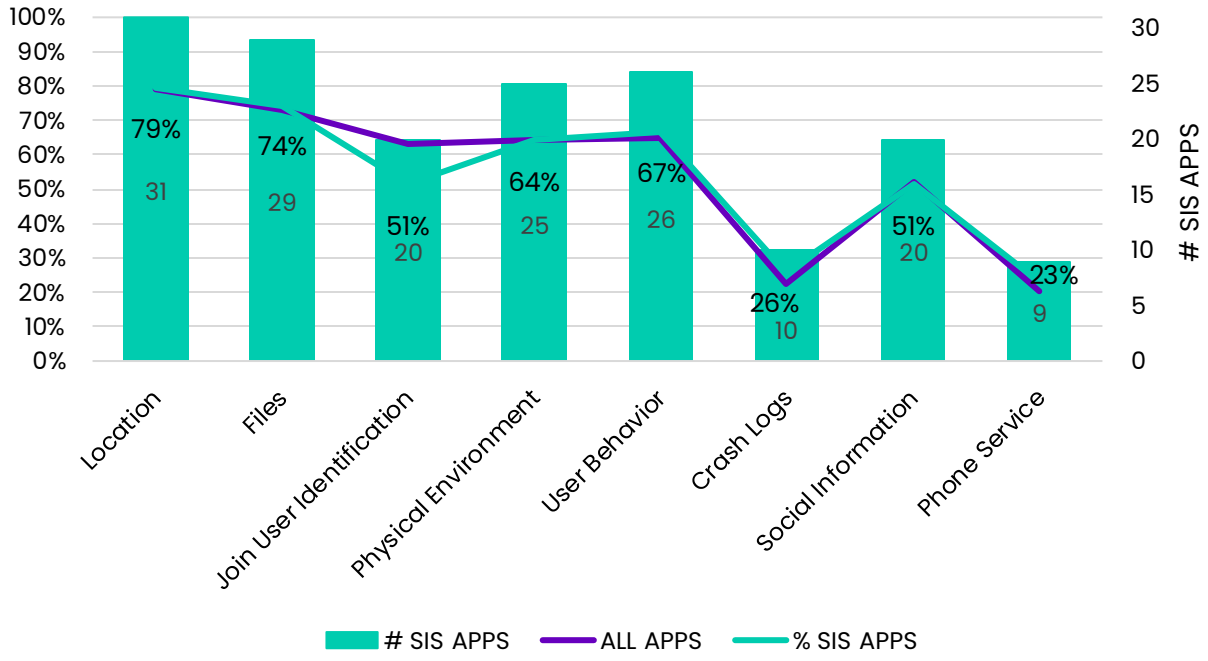


Figure 11.9 — Permissions - SMS Apps

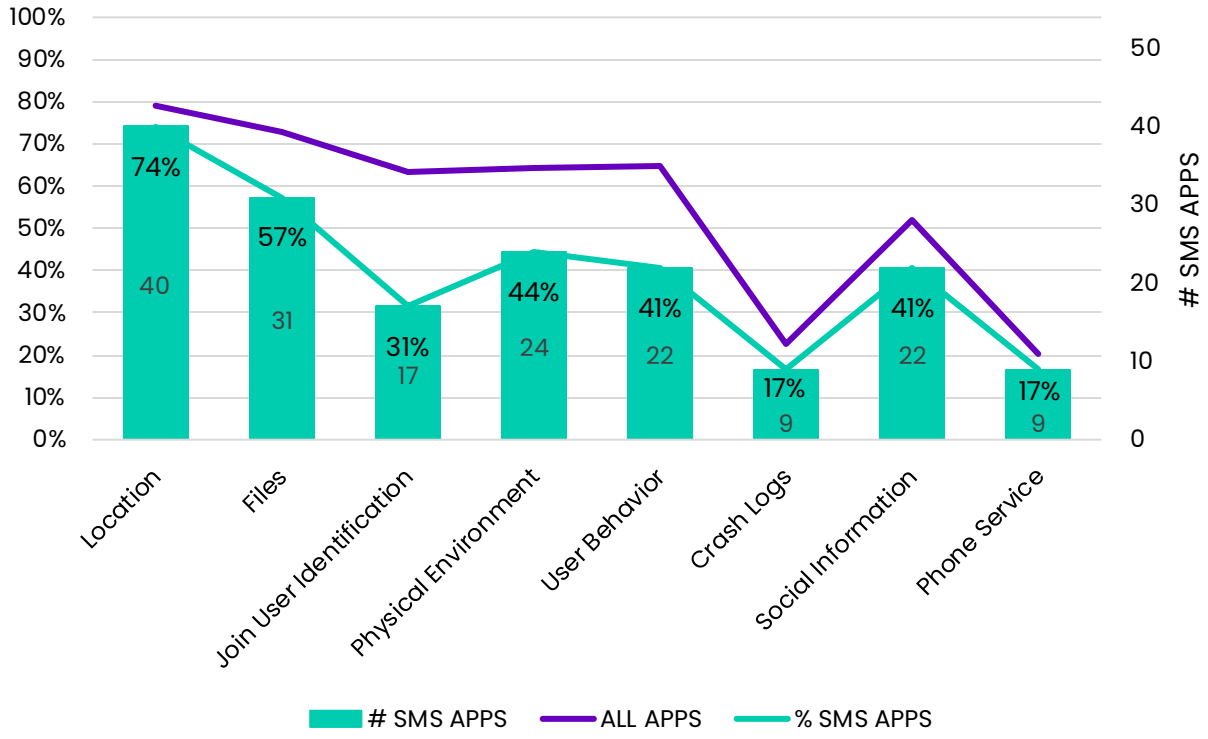


Figure 11.10 — Permissions - SP Apps

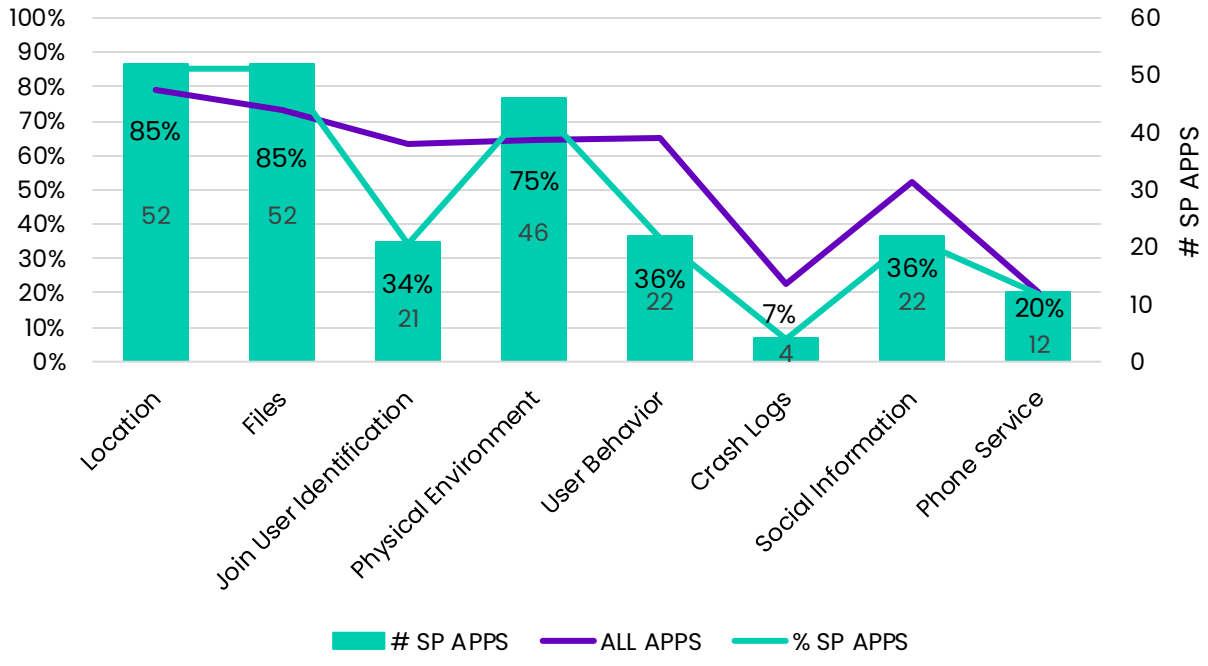


Figure 11.11 — Permissions - SSO Apps

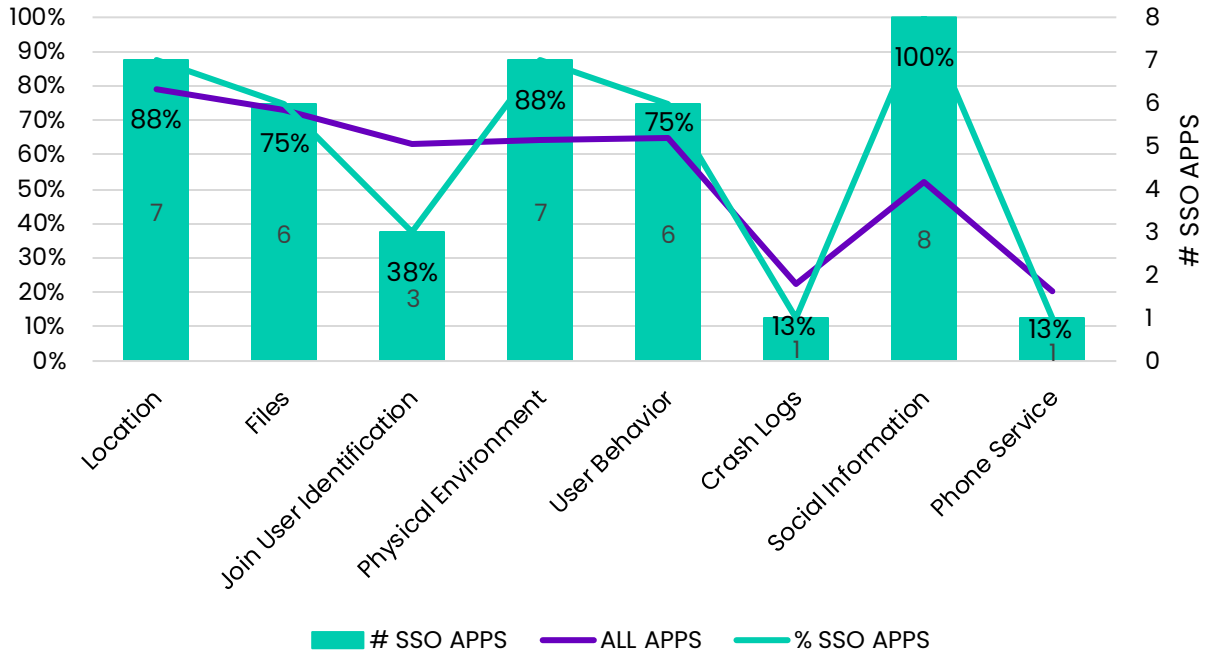


Figure 11.12 — Permissions - ST Apps

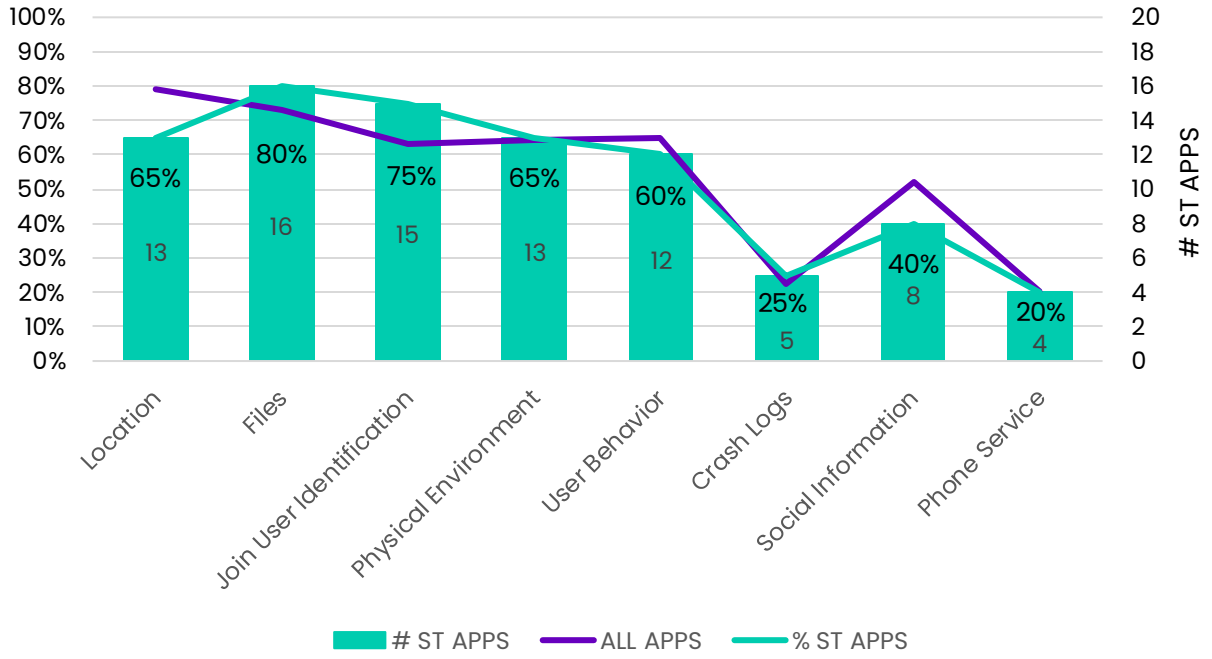


Figure 11.13 — Permissions - STS Apps

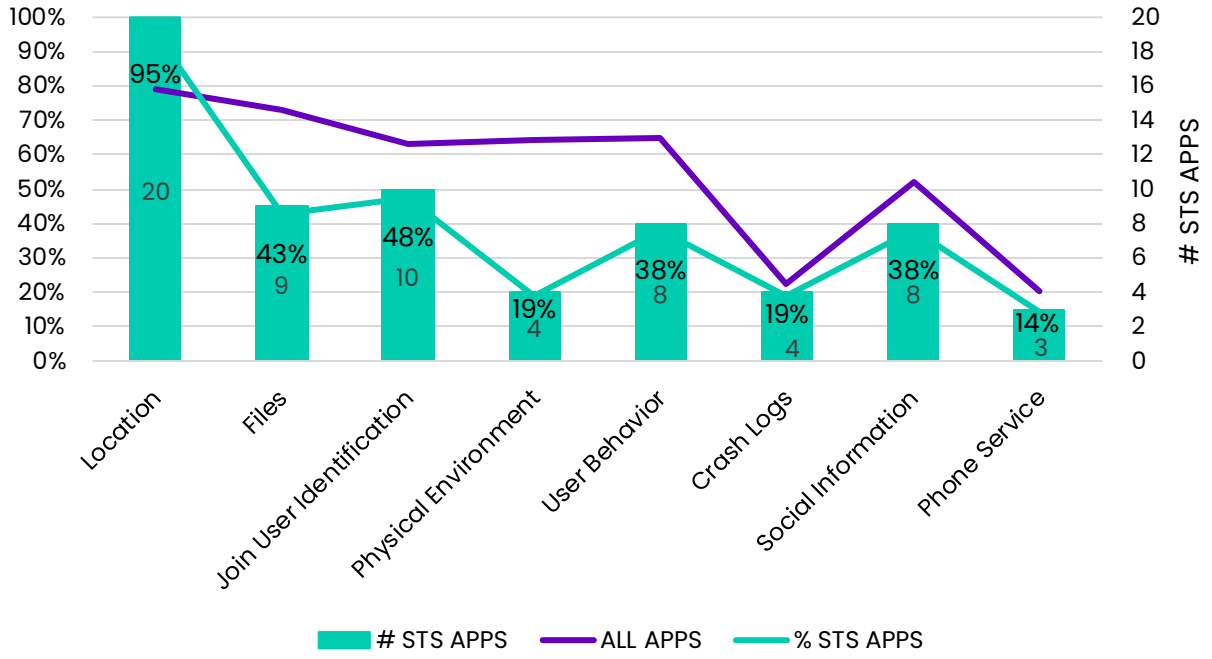
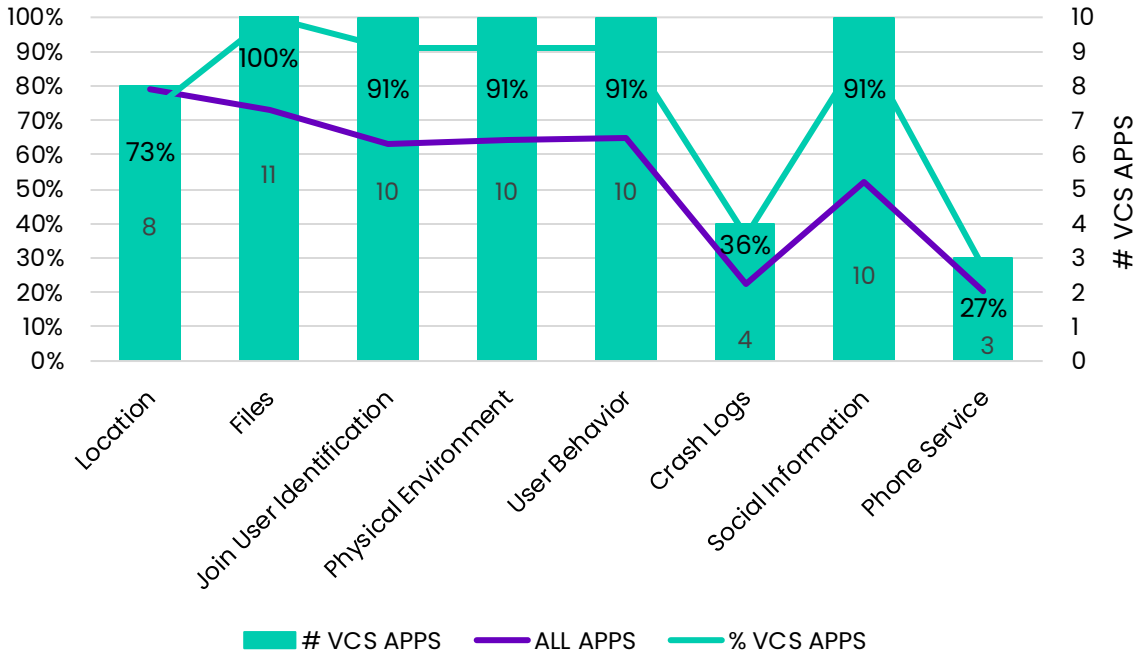


Figure 11.14 — Permissions - VCS Apps



12 Appendix E: Apps with Observed Retargeting Ads

App Name	OS	App Developer
KidzSearch	iOS	KidzSearch.com
Flight Pilot Simulator 3D!	iOS	Fun Games for Free
Pixlr — Photo Collages, Effect	iOS	Inmagine Lab Pte. Ltd
AllSides	Android	AllSides LLC
AllSides - Balanced News	iOS	AllSides LLC
Amazon Shopping	Android	Amazon
Amazon Shopping	iOS	Amazon
American Heritage English	Android	MobiSystems, Inc.
AP News	iOS	The Associated Press
AP News	Android	The Associated Press
BBC News	Android	British Broadcasting Corporation
BBC News	iOS	British Broadcasting Corporation
Blooket - Brain teasers games	Android	Adapted Brain
Brain it On!	iOS	Orbital Nine
Breathe+ Breathing Exercises	iOS	DynamicAppDesign, Inc.
Chess HD ·	iOS	Optime Software
Chicago Tribune	Android	Tribune Publishing Company
Chicago Tribune	iOS	Tribune Publishing Company
Clarion Ledger eNewspaper	Android	Gannett Co., Inc.
CNN Breaking US & World News	iOS	Warner Media Companies
CNN: Breaking US & World News	Android	Warner Media Companies
Colorfy	iOS	Wildlife Studios
COVID Coach	Android	U.S. Department of Veterans Affairs
COVID Coach	iOS	U.S. Department of Veterans Affairs
Cymath - Math Problem Solver	Android	Cymath LLC

Cymath - Math Problem Solver	iOS	Cymath LLC
Delta Mathematics	Android	deltaco
Delta Mathematics	iOS	deltaco
Dictionary - Merriam-Webster	Android	Merriam-Webster, Inc.
Dictionary.com English Word Me	Android	Dictionary.com, LLC
Dictionary.com: English Words	iOS	Dictionary.com, LLC
Encyclopædia Britannica	iOS	Encyclopaedia Britannica, Inc.
Flight Pilot: 3D Simulator	Android	Fun Games for Free
Happy Color® – Color by Number	Android	X-FLOW LTD
Happy Color® – Color by Number	iOS	X-FLOW LTD
Imgflip: Make Memes & GIFs	Android	Imgflip LLC
Issuu: magazine & books	Android	Issuu Inc.
Journal Star	Android	Lee Enterprises Inc.
Journal Star	iOS	Lee Enterprises Inc.
KEVN Black Hills FOX News	iOS	Gray Television, Inc.
KEVN Black Hills FOX News	Android	Gray Television, Inc.
Key Ring Reward Cards	iOS	InMarket Media LLC
Key Ring: Your mobile wallet	Android	InMarket Media LLC
Kids Doodle - Color & Draw	Android	Beauty Photo, LLC
Kids Doodle - Draw Sketch	iOS	Beauty Photo, LLC
KidzSearch Safe Search Engine	Android	KidzSearch.com
KOTA News	iOS	Gray Television, Inc.
KOTA Territory News	Android	Gray Television, Inc.

KQED	iOS	KQED Inc.
Merriam-Webster Dictionary	iOS	Merriam-Webster, Inc.
Omaha World-Herald Omaha.com	Android	Lee BHM Corp.
Omaha World-Herald Omahacom	iOS	Lee BHM Corp.
Paint.ly - Color by Number	Android	Newque Tech Limited
Paint.ly Color by Number Game	iOS	Newque Tech Limited
Pixlr — Photo Editor	Android	Inmagine Lab Pte. Ltd
Pocket: Save. Read. Grow.	Android	Mozilla Corporation
Rapid City Journal	Android	Lee Enterprises Inc.
Rapid City Journal	iOS	Lee Enterprises Inc.
Run Marco!	iOS	Allcancode, Inc.
SBLive Sports	Android	SBLive Sports
SBLive Sports	iOS	SBLive Sports
Scientific American	Android	Springer Nature America, Inc.
ScoreStream High School Sports	Android	ScoreStream Inc.
ScoreStream Sports Scores	iOS	ScoreStream Inc.
Semantle: Daily Word Game	Android	David Turner
Semantle: Daily Word Game	iOS	David Turner
Sesame Street	iOS	Sesame Workshop
St. Louis Post-Dispatch	Android	Lee Enterprises Inc.
St. Louis Post-Dispatch	iOS	Lee Enterprises Inc.
Target	Android	Target
Target	iOS	Target
The Weather Channel	iOS	TWC Product and Technology, LLC dba The Weather Company
The Weather Channel - Radar	Android	TWC Product and Technology, LLC dba The Weather Company
Today's Top News - USA TODAY	iOS	Gannett Co., Inc.
TurtleDiary	Android	TurtleDiary

Twitter	Android	Twitter
Twitter	iOS	Twitter
USA TODAY	Android	Gannett Co., Inc.
Weather Underground: Local Map	iOS	IBM
Youtube	Android	Google LLC
Youtube: Watch, Listen, Stream	iOS	Google LLC
Central Dauphin Schools	iOS	Anthology (Blackboard)
Hays USD 489, KS	Android	Apptegy, Inc.
Alexandria City Public Schools	iOS	Anthology (Blackboard)
Alexandria City Public Schools	Android	Anthology (Blackboard)
Atlanta Public Schools (APS)	Android	Anthology (Blackboard)
Atlanta Public Schools (APS)	iOS	Anthology (Blackboard)
Berkeley County Schools (WV)	Android	Anthology (Blackboard)
Berkeley County Schools (WV)	iOS	Anthology (Blackboard)
Birmingham City Schools	Android	Anthology (Blackboard)
Birmingham City Schools	iOS	Anthology (Blackboard)
Blue Valley Schools KS	iOS	Anthology (Blackboard)
Central Dauphin Schools	Android	Anthology (Blackboard)
East Allen County Schools	iOS	Apptegy, Inc.
Fort Smith PS Athletics	Android	Mascot Media, LLC
Hays CISD	Android	Anthology (Blackboard)
Hays CISD	iOS	Anthology (Blackboard)
Hays USD 489, KS	iOS	Apptegy, Inc.
Henry County Schools (GA)	Android	Anthology (Blackboard)

Hudson City Schools - Ohio	iOS	Anthology (Blackboard)
Hudson City Schools - Ohio	Android	Anthology (Blackboard)
Jamestown 1-ND	iOS	Anthology (Blackboard)
Jefferson West USD 340	iOS	Apptegy, Inc.
Jefferson West USD 340	Android	Apptegy, Inc.
KHSAA/Riherds Scoreboard	iOS	Frank Riherd
Madison County Schools	Android	Anthology (Blackboard)
Madison County Schools	iOS	Anthology (Blackboard)
Montgomery Public Schools	Android	Anthology (Blackboard)
Oakes Public Schools	iOS	Anthology (Blackboard)
Oakes Public Schools	Android	Anthology (Blackboard)
OCPS	Android	Intrado Corporation
OCPS	iOS	Intrado Corporation
Ohio County Schools, WV	Android	Apptegy, Inc.
Ohio County Schools, WV	iOS	Apptegy, Inc.
Palm Beach County School Dist	Android	Intrado Corporation
Palm Beach County School Dist	iOS	Intrado Corporation
Plant City High School	Android	Heather Hanks
Plant City HS	iOS	Heather Hanks
Prince George's County PS	iOS	Anthology (Blackboard)
Prince George's County PS	Android	Anthology (Blackboard)
Providence Schools	Android	Anthology (Blackboard)
Ritenour Schools	Android	Anthology (Blackboard)
Ritenour Schools	iOS	Anthology (Blackboard)
Westover Christian Academy	Android	Apptegy, Inc.
Westover Christian Academy	iOS	Apptegy, Inc.

AntiStress & Relaxing Games	iOS	Moreno Maio
Newsy - Video News	iOS	E.W. Scripps Company
Planner 5D: Interior Design	iOS	Planner5D, UAB
OCD.app - Anxiety Mood & Sleep	iOS	GG Apps
Marshall Public Schools, MO	iOS	Apptegy, Inc.