2022 K-12 EdTech Benchmark Findings Report 2:

School Technology Practices & 3rd Party Certifications Analysis

June 27, 2023

INTERNET SAFETY LABS

Acknowledgements

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

Contributors

Writing: Lisa LeVasseur, Daniella Doern

Researchers: Alyssa Bernardino, Bryce Simpson, Daniella Doern, Lisa LeVasseur, Irene Knapp

Quantitative Analysis & Data Visualization: Bryce Simpson, Steven Turnbull, George Vo

Design: Andrea Ausland

1 Table of Contents

2 Executive Summary

2.1 Scope

This is the second findings report from Internet Safety Lab's 2022 US K12 EdTech safety benchmark, which 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.

50 states + D of C
663 schools
455,882 students
1,722 apps
117,000+ data points

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.

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 & Recommendations

2.2.1 School Technology Practices

1. Schools don't systematically provide **technology notice and consent.**
    a. While notice and consent (aka "notice and choice") is a mainstay in most privacy law, there is no mandatory requirement for EdTech in schools.
    b. Only **45% of schools provide a technology notice** clearly listing all technology used by students (Figure 6.1).
        i. ISL researchers had difficulty in finding complete and accurate lists of all the technologies used by students for a school or district. It's likely that parents in the US are having a very difficult time knowing all the technologies their children are using for school.
    c. Only **14% of schools provided the ability** for parents/students 18 years or older to **consent to technology use** (Figure 6.2).

d. Some schools may be over-applying the legal ability to consent on behalf of the students.
    i. ISL occasionally found school-consented-to technology lists containing in at least one case **hundreds** of websites/apps. The lists included "off the shelf" technologies that students provision and use independently of the school (or don't require a login at all).
    ii. ISL is not a legal expert, but in our opinion, LEAs cannot adequately consent on behalf of students for technologies with which the school has no actual relationship, and for which students can independently sign up for accounts or use without an account (i.e. "off the shelf" technologies).
    iii. ISL estimates that of all the technologies required or recommended by schools, **only 19.3% of them are licensed by the school/LEA**, and 80.7% are off the shelf technologies.
    iv. ISL recommends that LEAs **not consent** to long lists of technologies, as a standard practice.
    v. In specific, ISL recommends that LEAs **not consent** to off the shelf technologies—particularly technologies that are not designed for education or children. (As a reminder, 28% of the apps in our sample were technologies that are neither designed for educational purposes or for use by children.)
    vi. Because schools routinely—and reasonably--recommend and require technology that is not designed for children, **ISL continues to advocate that *all* software be made safe for all people regardless of age.**

2. Schools aren't performing vetting of all recommended technology, and when they do, it has mixed safety results.
    a. Only **29% of schools appeared to be vetting *all* technology** used by students (Figure 6.4).

b. **Schools with technology vetting had no difference at all in safety scores**; surprisingly, the score distribution was identical (Figures 6.9, 6.10).
c. Schools with technology vetting were **somewhat less likely to have ads** in apps 11.1% of schools vs. 16.1% of schools without vetting (Figure 6.13).
d. **Schools with technology vetting had worse (higher) school composite scores** (Figure 6.11) than schools without vetting. This is likely related to finding 2e.
e. Schools with technology vetting recommended/required 27.6% more apps on average than schools without any observed vetting.
    i. **Technology vetting may be providing a false sense of security.**

3. **Effectiveness of SOPIPA:** Note that these findings are not definitive due to the testing methodology but are included as possible trends for future validation.
    a. **Despite their intention to ban retargeting ads, SOPIPA-like laws are *not* 100% effective** (Figure 6.20).
    b. **SOPIPA-like laws do appear to be having a positive impact on reducing retargeting ads in EdTech.**
        i. States without SOPIPA laws were 84.8% more likely to have apps with retargeting ads than states with SOPIPA laws.
    c. **However, 25% of states with SOPIPA-like laws still had retargeting ads.** (Figure 6.19).
        i. The states were: Arkansas, Colorado, Georgia, Illinois, Kansas, Maryland, Maine, Michigan, North Carolina, Nebraska, Tennessee, Texas, and Virginia.
        ii. Since we tested such a small sample of schools, ISL believes that the actual percentage could approach 100% of all states with SOPIPA laws, due to the pervasive unsafe software development norms and the difficulty of enforcement. Further analysis is recommended.
4. SOPIPA-like laws seem to have a mixed effect on school technology use. Schools in states with SOPIPA-like laws:
    a. Are more likely to provide technology notice (Figures 6.14a, 6.14b).

b. Are less likely to offer opportunities for technology use consent (Figure 6.15).
c. Have somewhat fewer Do Not Use apps (Figure 6.16).
d. Have somewhat higher (worse) app composite scores than schools in states without SOPIPA like laws (Figure 6.17).

2.2.2 Third Party Certifications and Promises

5. As noted in Findings Report 1, Community Engagement Platform (CEP) apps were consistently some of the least safe apps in the sample. CEP apps are largely comprised of the commonly found "School Utility Apps"—the least safe apps in the sample.
    a. School Utility Apps (the majority of apps listed in Appendix B) should not be used by schools or school districts until they are overhauled for student safety.
    b. We opted to remove all the CEP apps from the analysis examining third party certifications and promises, given how much the apps' unsafe behaviors skewed the findings, and also due to the relatively low number of downloads for most of these apps.
    c. We strongly encourage third party certifiers and promises to exclude these apps until they are made safer.
        i. Currently iKeepSafe and Student Data Privacy Pledge are the two third party certifications/promises that include School Utility Apps (Appendix C).
6. Overall, after removing the CEP apps, **the set of apps with any certification or promise was safer** than the set of apps with no certifications or promises.
7. The set of apps with any type of *certification* had mixed safety results (Table 7.2c).
    a. They had no retargeting ads (excellent),
    b. But they had an **appreciably higher percent of Do Not Use (DNU) apps (63.4%) than the overall sample (54.6%)** *and* apps with *no* certification or promise (56.1%),
    c. The certified apps also had a higher percentage of ads in apps (16.2%) than the overall sample (15.2%), but lower than apps with no certification or promise (18.6%).

8. **COPPA Safe Harbor certified apps have more advertising than the overall sample, *and* apps without any certification, and are too frequently sharing student data with risky, large platforms like Facebook and Twitter:**
    a. They had a **higher percentage of ads** (21.6%) than the overall sample (15.2%) as well as apps without any certification or promise (18.6%).
    b. They had a **much higher percentage of DNU apps** (73.8%) than the overall sample (54.6%), and apps with no certification or promise at all (56.1%)
9. 1EdTech provides a proprietary privacy certification and their certified apps stood out with **a significantly lower percentage of DNU apps** (40.0% vs. 54.6% in the overall sample set), **no digital ads in the apps, and no retargeting ads**.
10. After removing the CEP apps, **apps with either of the two *promises* [Student Privacy Pledge or Student Data Privacy Consortium (SDPC)] performed better than the overall sample set (Table 7.2c)**.
    a. The Student Privacy Pledge had only 38.6% DNU scores, only 2.1% of apps had ads and only 2.1% had retargeting ads. While better than the overall sample, the presence of retargeting ads indicates room for closer monitoring of apps behavior.
    b. The SDPC apps had 53.9% DNU apps—somewhat less than the overall sample set—and only 8.0% of the apps had ads, and 2.3% of the apps had retargeting ads, both significantly better than the overall sample set.
11. **Certifications** seem to be **more effective** than **promises** at eliminating **retargeting ads** (Table 7.2c).
12. Apps with **promises** have **better safety scores** than the **certified apps**.
13. Apps with *vendor-asserted COPPA compliance* had mixed results when compared to the overall sample (Table 7.2c):
    a. The percentage of DNU apps was slightly higher (55.7%) than the whole sample (54.6%), but the percentage of apps with ads was lower (11.2% vs. 15.2%) as was the percentage of apps with retargeting ads (7.1% vs. 8.9%).

b. Somewhat surprisingly, vendor-asserted COPPA compliance seems to have a slight positive impact on (i.e. reduction of) the presence of ads and retargeting ads in apps.

Overall, we were generally encouraged by the effects of certifications and promises on app safety. The high percentage of DNU apps in the COPPA Safe Harbor certified apps is concerning, of course, and we hope that the ongoing publishing of our 2022 benchmark findings and data helps organizations (certifiers, schools, LEAs, etc.) navigate technology behavior risks more efficiently and effectively.

3 Glossary

3.1 Advertising

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

3.2 Contextual Advertising

Contextual advertising refers to digital advertising content based on characteristics of the publication site, not based on user behavior. This is in contrast to **retargeting advertising** (3.9).

3.3 EdTech

In this research, we use the term EdTech in a very broad manner to mean the collection of digital technologies (app, webservices, etc.) that K12 schools require or recommend students to use as a part of their educational process. We further define EdTech App Categories (3.2).

3.4 EdTech App Category

EdTech apps come in a very wide range of functionality and utility. We created an edtech typology to facilitate comparing like-to-like edtech apps. The categories are listed here and details on the typology can be found in Appendix A of Findings Report 1.

- 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)

3.5 ISL Safety Score

The ISL safety score was introduced in Findings Report 1 and conveys the overall safety of a mobile app. There are four possible score dispositions:

1. Unable to Test: which means we were unable to assign a score,
2. Some Risk: the safest of the three scores, meaning that there is some risk in the app,
3. High Risk: the middle of the three risk scores,
4. Do Not Use: the highest risk score assigned.

See Appendix A for more information.

3.6 K12 / K-12

K12 or K-12 is shorthand for kindergarten through twelfth grade, the full range of primary education for children in the US.

3.7 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.

3.8 Personally Identifiable Information (PII)

Personally identifiable information refers to any data which can in principle be joined to an individual person, with or without the use of additional data.

3.9 Retargeting Advertising

Retargeting refers to the capability to anonymously 'follow' consumers all over the Web. Retargeting ads are ads that rely on information that has followed the user from another site, based on the testing by our researchers. This is also referred to as "behavioral advertising", meaning ads are delivered in accordance with the user's observed [usually surveilled] behaviors.

3.10 School Composite Score

The school composite score is the weighted average of the scores of all scored apps used by a school multiplied by the total number of apps in use at the school. The higher the score, the riskier the overall technology portfolio being recommended/required by the school.

e.g. Riverdale High School uses 9 apps:

App	Score	Weight
App 1	Do Not Use	3
App 2	High Risk	2
App 3	High Risk	2
App 4	Do Not Use	3
App 5	Do Not Use	3
App 6	Do Not Use	3
App 7	Some Risk	1
App 8	Do Not Use	3
App 9	Unable to Test	Not included in average.

Riverdale High School's composite score = (((5 Do Not Use Apps * 3) + (2 High Risk Apps * 2) + (1 Some Risk app * 1) / 8 Scored Apps) * 9 Total Apps = 22.5

Note that the average school composite score across the entire US was 54.3. Thus, the fictitious Riverdale High School is performing *better* than the national average school composite score.

3.11 Student Data Privacy Consortium (SDPC)

SDPC provides LEAs with data privacy agreement templates, as well as a management platform to review, aggregate, and manage data privacy agreements between LEAs and EdTech vendors.

The Student Data Privacy Consortium is part of the Access 4 Learning Community:

"A4L's Student Data Privacy Consortium (SDPC) is an unique collaborative of schools, districts, divisions, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns. The Consortium also leverages work done by numerous partner organizations but focuses on issues being faced by "on-the-ground" practitioners."[1]

SDPC provides LEAs with data privacy agreement templates, as well as a management platform to review, aggregate, and manage data privacy agreements between LEAs and EdTech vendors.

3.12 Software Developer Kit (SDK)

SDKs are externally developed and maintained reusable software modules/functions that can be integrated and invoked by an app, seamlessly within the app source code. SDKs provide commonly used functionality that developers don't wish to develop from scratch.

From our Spotlight Report #1:

"Most mobile apps are built with SDKs, which provide app developers with prepackaged 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."

[1] Student Data Privacy Consortium website: https://privacy.a4l.org/privacy-community/

3.13 Student Online Personal Information Privacy Act (SOPIPA)

SOPIPA is a California law that was considered the gold standard for student data privacy protection and has been the model for regulation passed in 24 states (total) to date. One of the key provisions in the regulation is the prohibition of *targeted advertising*. A covered operator's app, website, or service may not knowingly:

(A) Engage in targeted advertising on the operator's site, service, or application, or (B) target advertising on any other site, service, or application when the targeting of the advertising is based upon any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service, or application described in subdivision[2]

NOTE: while California's SOPIPA regulation fails to clearly define the term "targeted advertising", it's understood to mean advertising that uses any personal [student] information to present ads to the user. Thus, the definition of *targeted advertising* here includes the ISL definition of *retargeting advertising.*

3.14 Third Party Certification

A third-party certification is an assessment of an EdTech app against a set of criteria. Two types of certifications were observed amongst the apps in this benchmark: (1) COPPA Safe Harbor certifications, and (2) proprietary privacy certifications.

3.15 Third Party Promise

A third-party promise is a legally binding promise or contract that an EdTech vendor makes on behalf of a particular technology/platform/app. Two types of promises were observed amongst the apps in this benchmark: (1) The Student Privacy Pledge 2020, or (2) Data Privacy Agreements or similar as facilitated by the Student Data Privacy Consortium.

4 Overview

In 2022, Internet Safety Labs conducted a US-wide K12 EdTech safety benchmark, collecting data on a random, representative sample of 13 schools in each of the

[2] California State Bill 1177 https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177

50 states and the District of Columbia, 663 schools in total, covering about 455,882 students. In that sample, 1,722 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 and their technology related behaviors.

Our focus in the benchmark was measuring safety risks in K12 EdTech apps. The ISL Safety Score, introduced in Findings Report 1, is a new product safety scoring rubric based on the observed and measured behavior of the apps themselves. Currently, the safety score reflects only the *privacy behavior of the app*; in the future, the safety score will include additional safety considerations.

This report is the second findings report for the 2022 EdTech Safety Benchmark data and covers two analyses not included in Findings Report 1: (1) an analysis of school technology practices, and (2) examining the sample set of apps through a lens of third-party certifications and "promises". This report includes findings on school practices relating to technology *notice*, *consent*, and *vetting*. We also examine the overall safety of technology in schools that perform some kind of vetting versus technology in schools without vetting. Additionally, we take a closer look at common third-party certifications such as COPPA Safe Harbor and "promises" like the Student Privacy Pledge as compared to the ISL safety scores for apps, to determine if there is a relationship between the certifications and promises and the ISL Safety Score.

This report also includes an analysis of app safety in states with SOPIPA-like regulations (which disallow retargeting advertising to students) to understand if the regulations impact the ISL Safety Scores and advertising found in the apps used in schools in those states.

4.1 Important Caveats

1. Apps in this study were off-the-shelf versions of apps, i.e. *not* provided by the schools. All the apps analyzed in the benchmark were publicly available /off-the-shelf versions of the apps. ISL did *not* have access to school versions of apps and thus the app scores to not reflect the school versions. However, we estimate that 80.7% recommended to students is in fact off-the-shelf technologies.

2. As noted in Findings Report 1, at least 28% of the apps in our sample were not designed for children.
3. In this report we compare the ISL Safety Score with external certifications and "promises" to calibrate the safety scoring rubric and understand how the various methods relate to each other. ISL is *not* commenting on or evaluating the efficacy of external certifications and "promises". In section 8 of this report, we compare apps that have received external certifications (such as COPPA Safe Harbor certification or signed the Student Privacy Pledge) with the ISL safety scores and other risky behaviors of the overall set of apps. This analysis calibrates the ISL safety scoring rubric relative to the external certifications and promises. This helps both ISL and external entities understand how to relate to each other.
4. To understand school and district technology behaviors, ISL relied on information found in the school and district websites. ISL did *not* confirm the information with the school/district.

4.2 Data Visualization Conventions in This Report

- A purple trend line in a chart always reflects the behavior of the overall sample.
- Dark grey trend lines represent the behavior of the subset of apps under analysis.
- When both lines are present in a chart, the percentage labels displayed apply to the dark grey line—the subset of apps under analysis.

5 Summary of Student Data Privacy Laws

The US has a confusing patchwork of federal and state laws that protect student data. This section provides a general overview of these laws and focuses on laws that protect information sharing through and by digital technology.

All the laws noted in this section protect children and could all be in effect at the same time in the K-12 EdTech context. Key terminology such as the definition of personal information, the age range of who is considered a child, and who is subject to the regulation varies amongst the laws.

To gain a better understanding of the relationships between the laws, it's important to understand *whose* behavior the law is attempting to regulate.

5.1 Federal Regulations

We found mention of the following federal laws on school or district while conducting our benchmark research. For educational and research purposes only, we present a brief high-level overview of all the federal laws protecting student data in K-12.

Table 5.1 Federal Laws Mentioned on School/District Websites

Federal Law	Brief Description of the Law's Intent
Children's Internet Protection Act (CIPA)	To protect children from accessing obscene or harmful content online by requiring schools to adopt and implement an internet safety policy that includes content filtering, monitoring online activities of minors, and providing training of appropriate online behavior training for students.
Neighborhood Children's Internet Protection Act (NCIPA)	To protect children by requiring all participating schools to install filtering software on all school devices to prevent children from accessing obscene or harmful content online.
Individuals with Disabilities Education Act (IDEA)	To protect all students by ensuring that all individuals with disabilities receive equal access to education.

Protection of Pupil Rights Amendment (PPRA)	To protect students' rights involving their participation in surveys; certain physical exams; the inspection of instructional materials; and the collection disclosure and use of personal information for marketing purposes.
Family Educational Rights Privacy Act (FERPA)	To protect students from the unauthorized disclosure of Personal Information within the student's educational records.
Children's Online Privacy Protection Act (COPPA)	To protect the Personal Information of children when the child uses any online service that is directed towards children.

Table 5.2 Scope of Relevant Regulations

Federal Laws	Whose behavior is being regulated	Federal Agency that enforces the law
CIPA, NCIPA	Only Schools & Libraries that receive special funding or participate in the E-rate program	Federal Communications Commission
IDEA, PPRA, FERPA	Only Schools/LEAs	Department of Education
COPPA	Any online business that is considered a "COPPA covered company."	Federal Trade Commission

Figure 5.1 below is a simplified visual representation of which entities are governed by each of the federal laws and which Agency oversees the law.

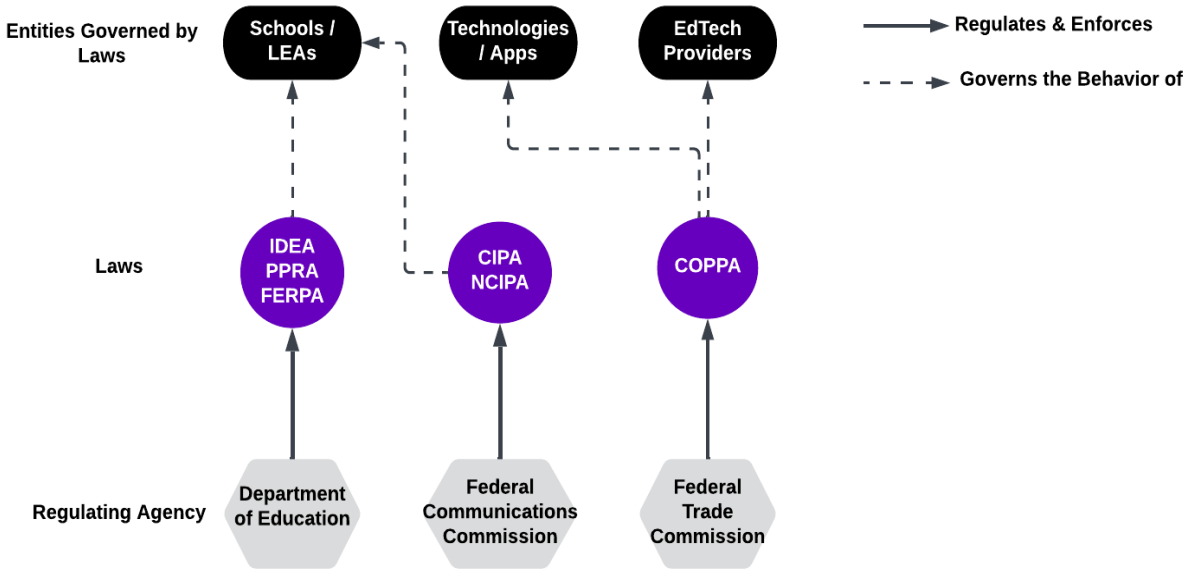


Figure 5.1

5.2 State Laws

In this report, we touch on findings related to federal regulation (COPPA), and also particular state regulation, described in this section.

Twenty-four states have modeled their state laws after California's Student Online Personal Information Protection Act ("CA SOPIPA"). For that reason, we present a summary of CA SOPIPA below.

SOPIPA isn't the only law that protects student privacy; it's important to keep in mind that other state statues may apply in your state.

For a more in-depth analysis on state regulations governing student privacy, please see the Parent Coalition for Student Privacy's 2019 report[3], the Center for Democracy & Technology's 2016 report[4], and summaries from the Future of Privacy Forum which include more recent laws.[5]

[3] State Student Privacy Laws | Parent Coalition for Student Privacy. (2022, December 5). https://studentprivacymatters.org/state-legislation/

[4] State Student Privacy Law Compendium. (2016, October 5). Center for Democracy and Technology. https://cdt.org/insights/state-student-privacy-law-compendium/

[5] Such as https://fpf.org/blog/connecticut-shows-you-can-have-it-all/

Table 5.3

CA SOPIPA
SOPIPA establishes privacy laws for EdTech Platforms that market their website, online service, or app for K-12 school purposes. The law itself refers to covered companies as Operators. An "Operator" is defined as an online service/product with actual knowledge that the site, service, or app is *used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes.*[6]This includes cloud computing services[7] but does not apply to general audience websites, online services, applications[8], even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications."[9] SOPIPA restricts the use of "*covered information*"[10] *but it does not restrict the use of "deidentified data."*[11] Operators must enter into contractual agreements with service providers prior to disclosing covered information. The contract must prohibit the covered information from being used for any other purpose other than the contracted service and prohibit further disclosure of the covered information to third parties. The contract must also require the service provider to implement and maintain reasonable security procedures and practices. Operators may not: • Engage in *targeted advertising* on the platform and/or provide *targeted advertising* on any other platform based upon any information, including covered information, that the EdTech Provider has acquired because of the student's use of the platform. • Sell a student's information. • Disclose covered information (unless it's disclosed for legal, regulatory, judicial, safety or operational improvement purposes). • Create student profiles (except for school purposes).

[6] SOPIPA, Cal. Bus. & Prof. Code §22584(a)
[7] SOPIPA, Cal. Bus. & Prof. Code §22584(h)
[8] SOPIPA, Cal. Bus. & Prof. Code §22584(m)
[9] SOPIPA, Cal. Bus. & Prof. Code §22584(m)
[10] SOPIPA, Cal. Bus. & Prof. Code §22584(i)
[11] SOPIPA, Cal. Bus. & Prof. Code §22584(f); SOPIPA, Cal. Bus. & Prof. Code §22584(g)

6 School Behaviors: Technology Notice, Consent, & Vetting Findings

This section contains the deep dive into the 663 schools' behavior with respect to technology notice, consent, and vetting.

6.1 Technology Notice

6.1.1 Data Collection Methodology

Initially, our researchers focused on whether schools were providing legal privacy notices, such as FERPA or COPPA notices. However, those notices didn't provide the information most needed by students and parents, namely, an accurate list of all the technology recommended or required for students. This kind of technology notice is not currently mandated by COPPA or SOPIPA laws but is frequently recommended as a best practice.[12] ISL believes that students and parents need and deserve to have this information. Since there is no mandated technology notice requirement, ISL defines "technology notice" as a complete list of all recommended/required technology for the school or the district.

Our research confirmed that schools don't always publicly provide these lists on their websites. In fact, our researchers had to carefully examine both the school and the district websites to find any kind of consolidated list of the technology being recommended or required by the school or district. The researchers also searched the Student Data Privacy Consortium (SDPC) site since it often held the most accurate and complete technology lists for the district.

Note that our determination of technology vetting presence was done without confirmation by the schools; it's possible that our identification process introduced inaccuracy in the results. Further analysis is required.

6.1.2 Technology Notice Findings

Fewer than half of the schools (45%) provided discoverable lists of technology required or recommended by the schools (Figure 6.1). Note that we did not measure the ease/difficulty of finding these lists, nor did we measure the accuracy of

[12] Student Online Personal Information Protection Act (SOPIPA) | Common Sense Media. (n.d.)., https://www.commonsensemedia.org/kids-action/about-us/our-issues/digital-life/sopipa

these lists. In general, locating comprehensive lists of technology was challenging, requiring multiple different search techniques as described earlier. Ultimately, we ended up with three distinct lists of technologies for each school: (1) a manually identified list of technologies that were clearly referenced either on the school or district website, (2) a "technology notice" which was a consolidated list of technologies which sometimes distinguished (3) approved technologies. Note also that we did not include technologies that were strictly for use by parents or teachers/administrators. The analysis in this section reflects the second category: a consolidated, single list of technology that the school or district posted.

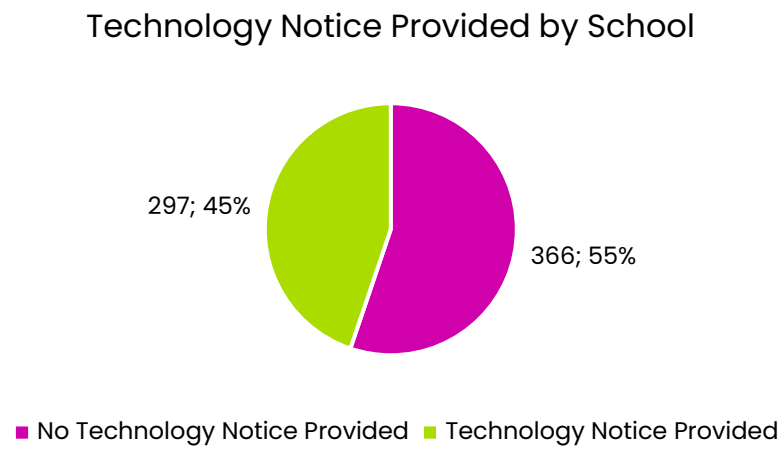


Figure 6.1

As mentioned in Findings Report 1, the researchers tried to identify which apps were required for students, but few of the school/district websites provided clear lists denoting required versus recommended. It's possible that this information is shared privately with students and parents through different channels. Such as it was, the researchers extrapolated "mandatory" technology based on whether it appeared in website menus (e.g., login links for MySchoolBucks on the school's homepage) or whether it was a technology likely to be licensed for use by the LEA, in which case, it was tagged as mandatory for students to use. (Please refer to Findings Report 1 for more details on the required vs. recommended technologies.)

Overall, it's likely that parents in the US are having an extremely difficult time knowing what technologies their children are using for school.

6.2 Technology Consent

6.2.1 Data Collection Methodology

Similar to technology notice, we're unaware of a federal or state mandate that requires schools to obtain actual parental or student consent for *all* technology use so the researchers had to search school websites, student handbooks, school board policies searching for any indication that parents/students could consent to or opt out of technology required by the school.

6.2.2 Technology Consent Findings

The ability to consent to student technology use is largely absent for both required and recommended EdTech, with 86% of the schools not providing any kind of consent option for technology use.

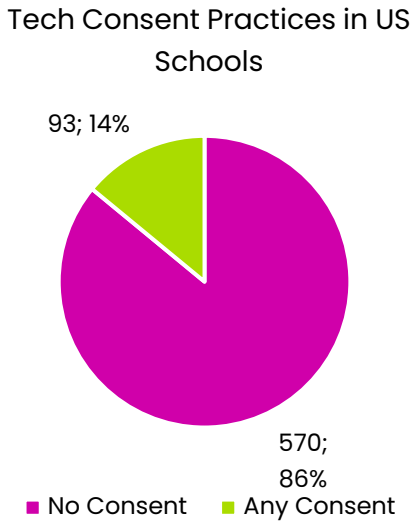


Figure 6.2

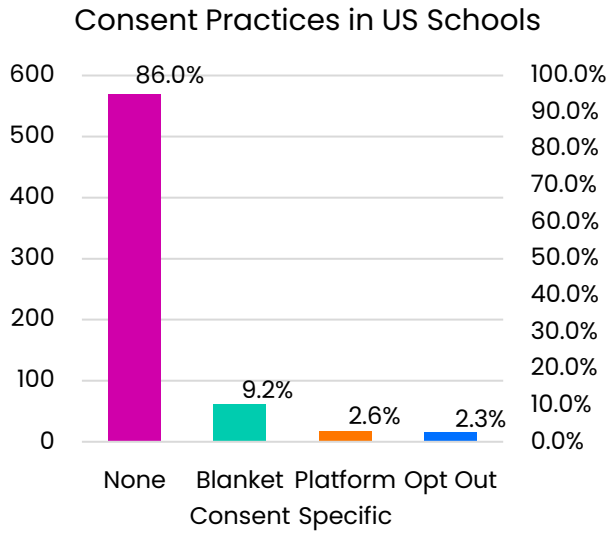


Figure 6.3

86.0% of schools did not provide parents [or students aged 18 or older] with an opportunity to consent to digital technologies in use by the school; 9.2% of schools offered the option to provide blanket consent for student technology use; 2.6% of schools offered the option to provide platform-specific consent, such as for Google Apps for Education; and 2.3% of schools offered the opportunity to opt out of technology.

So, in addition to not knowing what tech their children are required to use in school, parents are not being afforded methods to consent to or opt out of their child's use of technology. It should be noted that this is essentially by [regulatory]

design, since both FERPA[13] and COPPA have a broad "School Official" exception that allows the school to consent on behalf of the student for technology used for educational purposes. See Figure 6.2.2.1 for illustrations of the kinds of consent for the technologies studied in the benchmark. We identify three key types of consent: (1) LEA facilitated user consent, (2) DIY user consent, and (3) LEA provided consent OR legal exception [as in COPPA and FERPA].

LEA facilitated consent is the consent we saw in 14% of the schools (represented by the blue dashed line in the figure). Note that we include technologies provided by the school used strictly by parents/guardians in the diagram. *DIY user consent* means the student or guardian enrolled in and consented to a technology service themselves, completely outside of the school's knowledge or participation (represented by the blue solid line in the figure).

The most intriguing finding relates to the use of *LEA provided consent* for off the shelf and non-education specific technologies (solid green line in the figure).

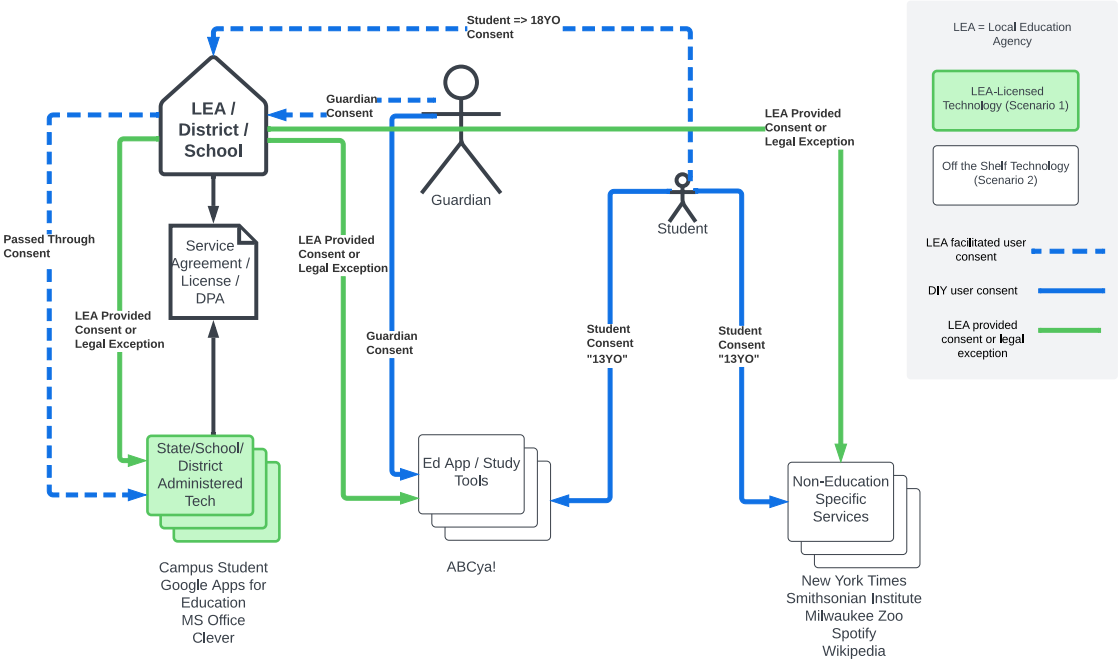
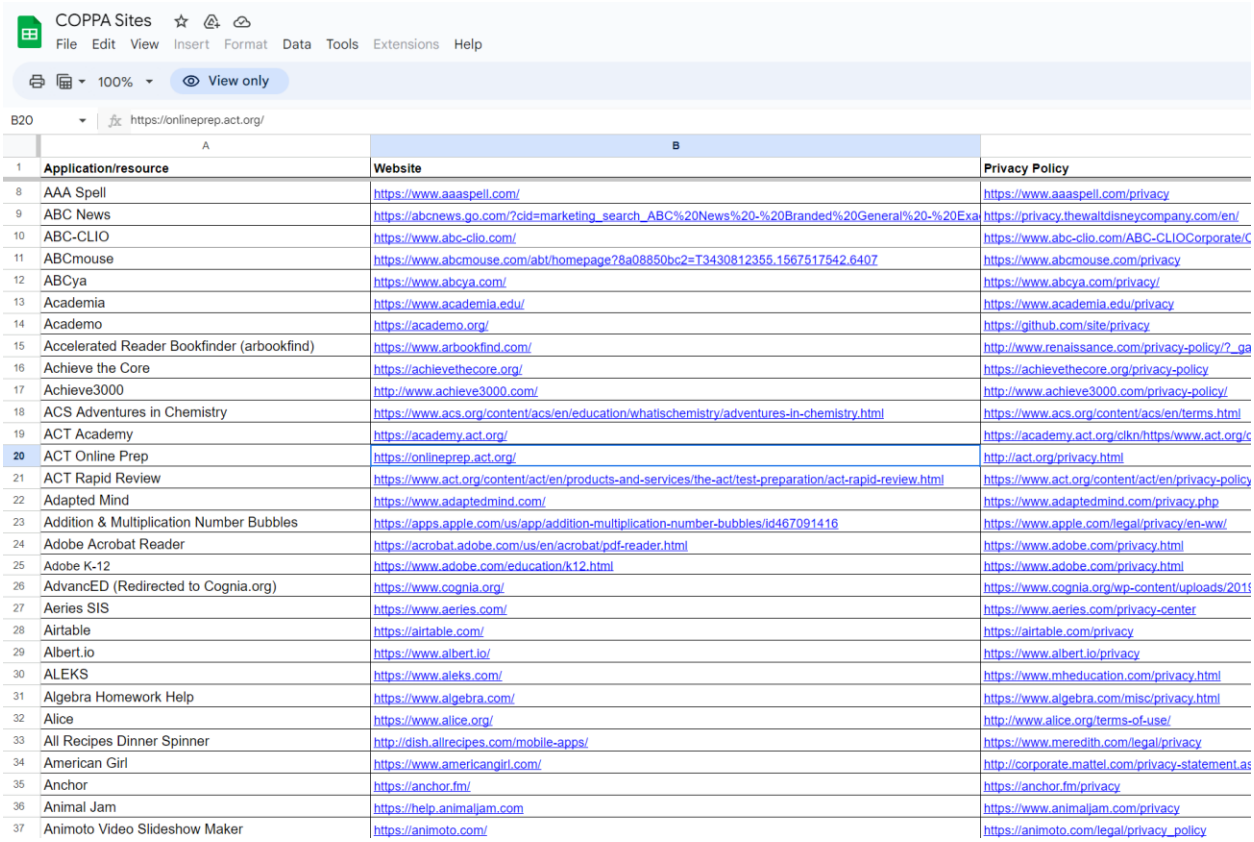


Figure 6.2.2.1 Observed Consent Practices

[13] See Family Educational Rights and Privacy Act (FERPA), and FERPA Exceptions—Summary (ed.gov)

6.2.3 Schools Consenting on Student Behalf

Our researchers encountered instances where the LEA provides a list of technologies along with links to their privacy policies and/or terms of service, and indicates that the school is consenting to use these services [under COPPA] on behalf of the student. ISL found that the lists can—and do—include "off the shelf" technologies or websites which the student accesses independently of the school or school-provisioned accounts. Examples include ABC News and American Girl websites as can be seen in Figure 6.2.3.1 below from the COPPA consented app list of 754 apps from Norfolk Public Schools in Virginia.[14]



COPPA Sites

File Edit View Insert Format Data Tools Extensions Help

100% View only

B20 https://onlineprep.act.org/

	A	B	
1	**Application/resource**	**Website**	**Privacy Policy**
8	AAA Spell	https://www.aaaspell.com/	https://www.aaaspell.com/privacy
9	ABC News	https://abcnews.go.com/?cid=marketing_search_ABC%20News%20-%20Branded%20General%20-%20Exa	https://privacy.thewaltdisneycompany.com/en/
10	ABC-CLIO	https://www.abc-clio.com/	https://www.abc-clio.com/ABC-CLIOCorporate/C
11	ABCmouse	https://www.abcmouse.com/abt/homepage?8a08850bc2=T3430812355.1567517542.6407	https://www.abcmouse.com/privacy
12	ABCya	https://www.abcya.com/	https://www.abcya.com/privacy/
13	Academia	https://www.academia.edu/	https://www.academia.edu/privacy
14	Academo	https://academo.org/	https://github.com/site/privacy
15	Accelerated Reader Bookfinder (arbookfind)	https://www.arbookfind.com/	http://www.renaissance.com/privacy-policy/?_ga
16	Achieve the Core	https://achievethecore.org/	https://achievethecore.org/privacy-policy
17	Achieve3000	http://www.achieve3000.com/	http://www.achieve3000.com/privacy-policy/
18	ACS Adventures in Chemistry	https://www.acs.org/content/acs/en/education/whatischemistry/adventures-in-chemistry.html	https://www.acs.org/content/acs/en/terms.html
19	ACT Academy	https://academy.act.org/	https://academy.act.org/clkn/https/www.act.org/c
20	ACT Online Prep	https://onlineprep.act.org/	http://act.org/privacy.html
21	ACT Rapid Review	https://www.act.org/content/act/en/products-and-services/the-act/test-preparation/act-rapid-review.html	https://www.act.org/content/act/en/privacy-policy
22	Adapted Mind	https://www.adaptedmind.com/	https://www.adaptedmind.com/privacy.php
23	Addition & Multiplication Number Bubbles	https://apps.apple.com/us/app/addition-multiplication-number-bubbles/id467091416	https://www.apple.com/legal/privacy/en-ww/
24	Adobe Acrobat Reader	https://acrobat.adobe.com/us/en/acrobat/pdf-reader.html	https://www.adobe.com/privacy.html
25	Adobe K-12	https://www.adobe.com/education/k12.html	https://www.adobe.com/privacy.html
26	AdvancED (Redirected to Cognia.org)	https://www.cognia.org/	https://www.cognia.org/wp-content/uploads/201
27	Aeries SIS	https://www.aeries.com/	https://www.aeries.com/privacy-center
28	Airtable	https://airtable.com/	https://airtable.com/privacy
29	Albert.io	https://www.albert.io/	https://www.albert.io/privacy
30	ALEKS	https://www.aleks.com/	https://www.mheducation.com/privacy.html
31	Algebra Homework Help	https://www.algebra.com/	https://www.algebra.com/misc/privacy.html
32	Alice	https://www.alice.org/	http://www.alice.org/terms-of-use/
33	All Recipes Dinner Spinner	http://dish.allrecipes.com/mobile-apps/	https://www.meredith.com/legal/privacy
34	American Girl	https://www.americangirl.com/	http://corporate.mattel.com/privacy-statement.as
35	Anchor	https://anchor.fm/	https://anchor.fm/privacy
36	Animal Jam	https://help.animaljam.com	https://www.animaljam.com/privacy
37	Animoto Video Slideshow Maker	https://animoto.com/	https://animoto.com/legal/privacy_policy

Figure 6.2.3.1

Figure 6.2.3.2 shows the consent notice with the pertinent language highlighted in yellow.

[14] We alerted Norfolk Public Schools about this finding prior to publication of this report.

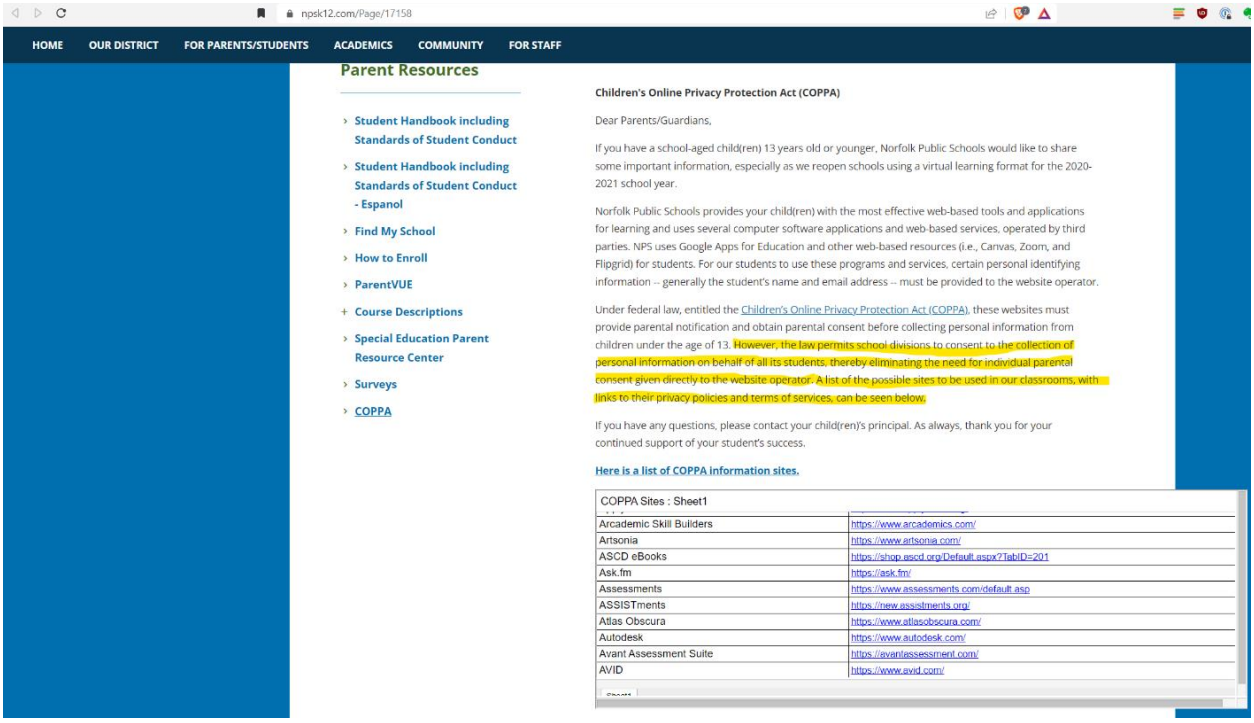


Figure 6.2.3.2 Norfolk School District COPPA Consent

To be clear, our intention isn't to be critical of LEAs, whom we are certain are doing the best they can with their limited resources. Our point is that the legal obligations of consent are tricky under the best of circumstances. The FTC recognizes the challenges and has developed this list of guidance for schools https://www.ftc.gov/business-guidance/blog/2020/04/coppa-guidance-ed-tech-companies-and-schools-during-coronavirus which includes this:

> **Is there any advice for schools that are using ed tech services**? Keep in mind that, because COPPA applies only to operators of commercial websites and services, it generally does not impose obligations directly on schools. Nevertheless, as schools and school districts move to remote learning, they should consult with their attorneys and information security specialists to review the privacy and security policies of the ed tech services they use. Schools or school districts should decide whether a particular site's or service's privacy and information practices are appropriate, rather than delegating that decision to the teacher. Also, the school or school district should give parents a notice of the websites and online services whose collection they have consented to on behalf of the parent. In deciding which online technologies to use with students, a school should be careful to understand how an operator will collect, use, and disclose personal information from its students. Among the questions that a school should ask potential operators are:
>
> - What types of personal information will you collect from students?
> - How do you use this personal information?

- Do you use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, do you use students' personal information in connection with generating targeted advertising, or building user profiles for commercial purposes not related to the provision of the online service? If so, the school cannot consent on behalf of the parent.
- Do you let the school review and have deleted the personal information collected from their students? If not, the school cannot consent on behalf of the parent.
- What measures do you take to protect the security, confidentiality, and integrity of the personal information that you collect?
- What are your data retention and deletion policies for children's personal information?

While ISL is not a legal expert**, in our opinion, schools and technology vendors cannot support the highlighted item for off the shelf technologies with which the school has no actual relationship, and for which students can independently sign up for accounts—or use without an account.**

For these reasons, ISL continues to advocate for technology that is safe to use by everyone, regardless of age.

Key Finding: it's clear that schools continue to struggle with knowing best practices for technology notice and consent.

6.3 Technology Vetting

6.3.1 Data Collection Methodology

As above, the search for evidence of technology vetting was performed by examining the school and district websites. We were looking for evidence that *all* technology (whether recommended or required) underwent rigorous student data privacy screening. It's likely that all schools are screening technology that is licensed by the school or district, i.e. there are likely to be supplier qualification requirements of some sort. We were, however, looking for more explicit vetting for student data privacy in *all* technology choices. Our researchers reviewed school board documents, supplier agreements, and general IT practices and policies to find any reference or evidence of a rigorous technology vetting program, especially relating to student data handling. The following are the practices that counted as evidence of technology vetting:

1. Vetting through the use of Student Data Privacy Consortium (SDPC) legal agreements.

2. Undisclosed/unpublished but explicitly mentioned technology approval/vetting practices.
3. District-specific, published vetting practices and procedures.
4. State mandated vetting, as prescribed in state statute.
5. COPPA vetting, typically meaning that the school requires technology vendors to be COPPA compliant, and the school has evaluated and stored privacy policies for technologies for students. NOTE: often this type of "vetting" leads to the consent problem noted in section 6.2.
6. LearnPlatform vetting of technology.
7. 1EdTech vetting of technology.
8. Requiring all school recommended/required EdTechnologies to sign the Student Privacy Pledge.

If we found a reference to any of the above on the school or district website, we recorded it as a school that vetted technology.

6.3.2 Technology Vetting Findings

Most (71%) of the schools in the US are NOT systematically vetting ALL technology recommended or required for students—at least not in a readily apparent manner.

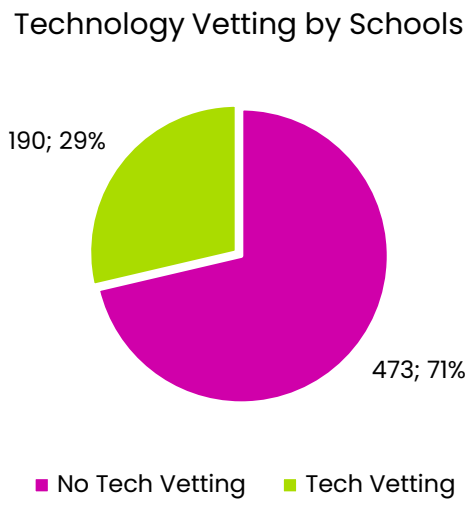


Figure 6.4

We further observed that occasionally (1.7% of the schools) (11 schools in total) schools had more than one type of vetting in evidence.

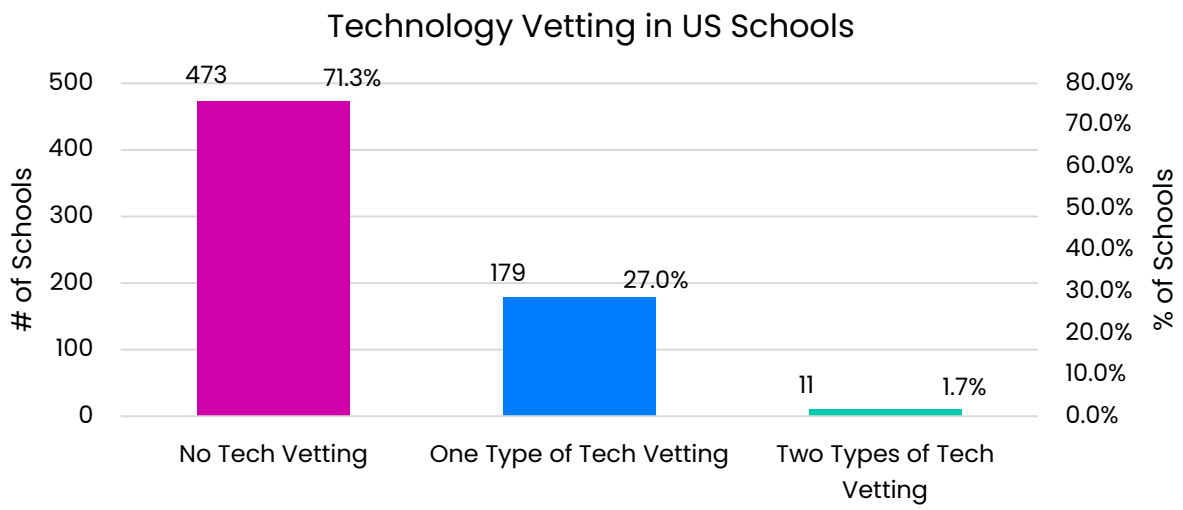


Figure 6.5

6.3.2.1 Types of Technology Vetting

Of the schools that vet technology, we observed eight types of vetting (Figures 6.6a and 6.6b). The use of the Student Data Privacy Consortium tools was the most prevalent type of vetting, used by 34% of the schools that perform any kind of vetting. Proprietary/unpublished vetting practices were the second largest category with 26% of schools that perform technology vetting.

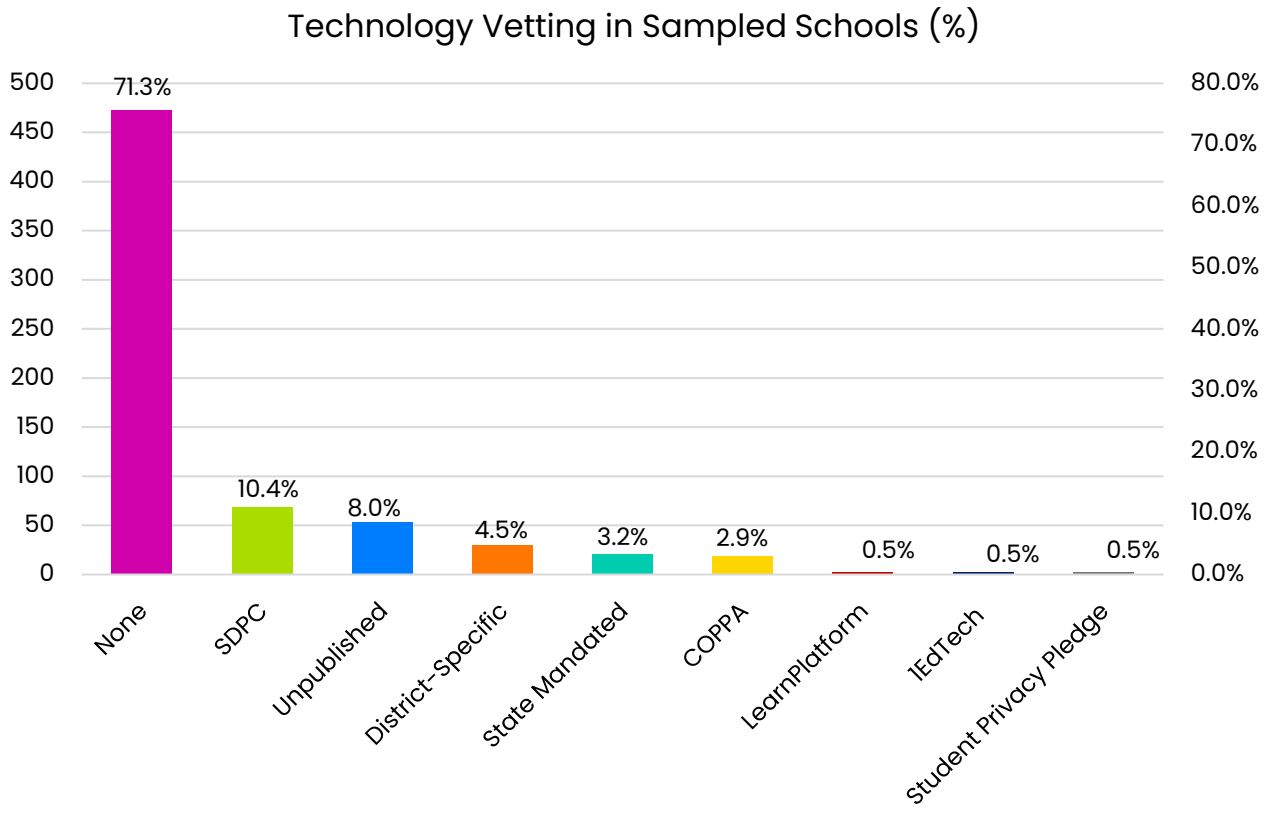


Figure 6.6a

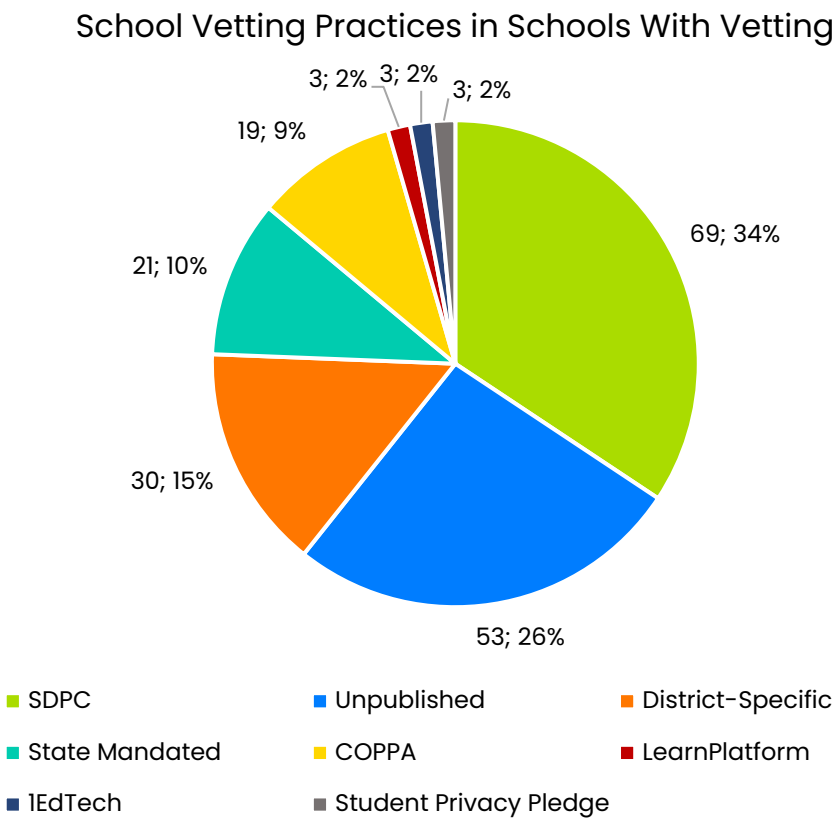


Figure 6.6b

6.3.2.2 Technology Vetting Efficacy

We were interested in understanding if the schools that had technology vetting practices had safer technology. Figure 6.7 below compares the number of recommended or required apps for each ISL Safety Score between schools that do and do not have technology vetting.

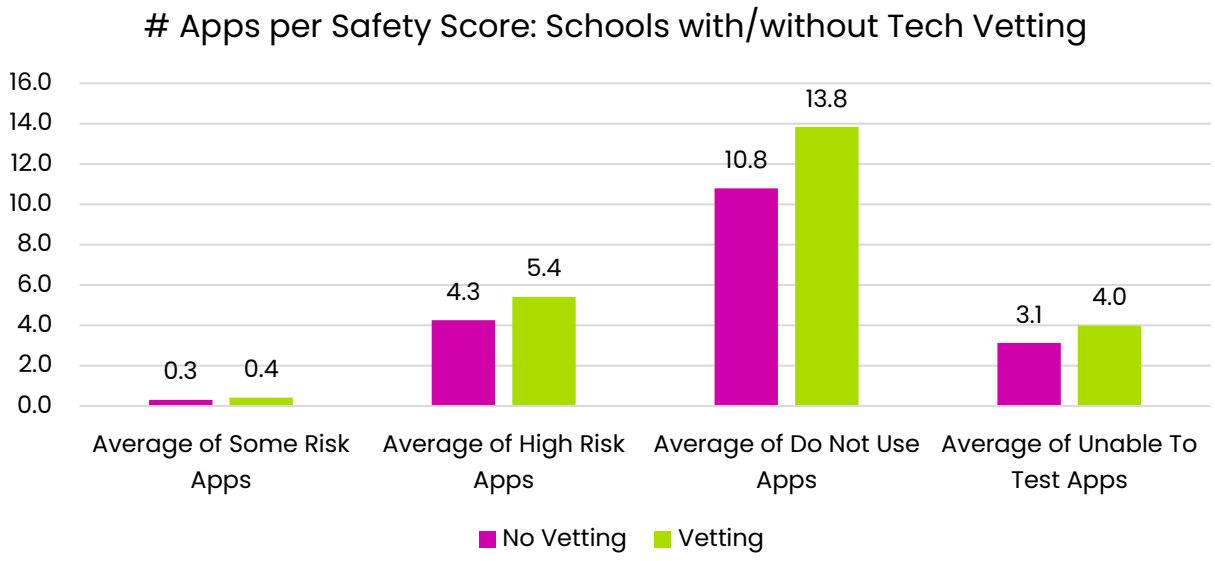


Figure 6.7

Surprisingly, schools with vetting practices recommend or require *more* apps in each safety bucket compared to schools without tech vetting. This is positive for Some Risk apps, but it is not good for High Risk and Do Not Use apps. *The average number of apps per school scored Do Not Use is 27.8% higher for schools with vetting than those without.* These findings could be simply because schools with vetting had a higher number of apps than schools without vetting. ***It's possible that the presence of vetting is giving schools a false sense of security about technology, which motivates them to require/recommend more technology.***

Indeed, as Figure 6.8 shows, schools with any kind of vetting *did* have on average 27.6% more recommended/required apps than schools without any vetting.

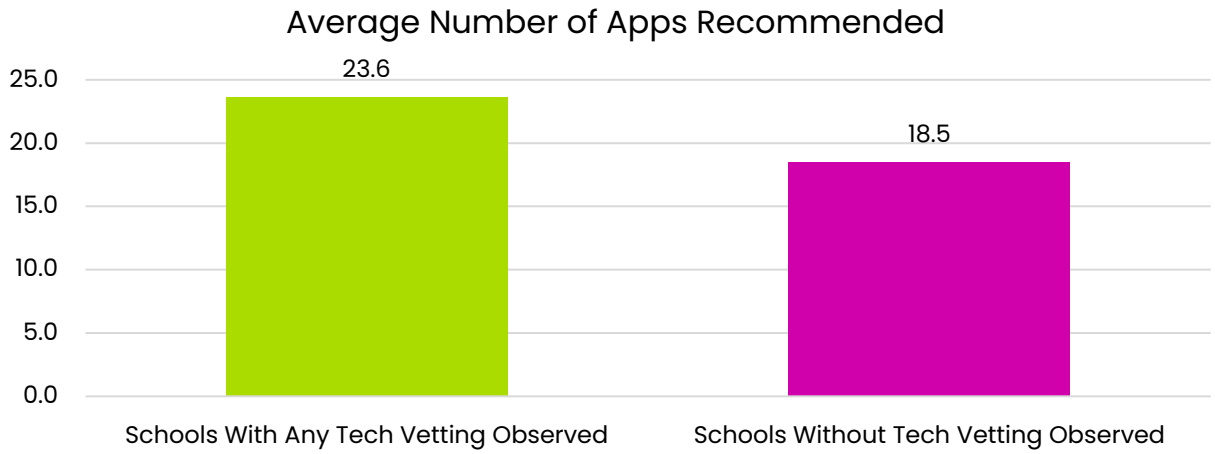


Figure 6.8

For a fairer score comparison, we looked at the percentages of apps in each of the app score categories for schools with and without vetting. To our further surprise, the proportions were *identical* across schools with vetting and schools without (see Figures 6.9 and 6.10 below). ***This suggests that there is no difference seen by schools with some form of vetting.***[15]

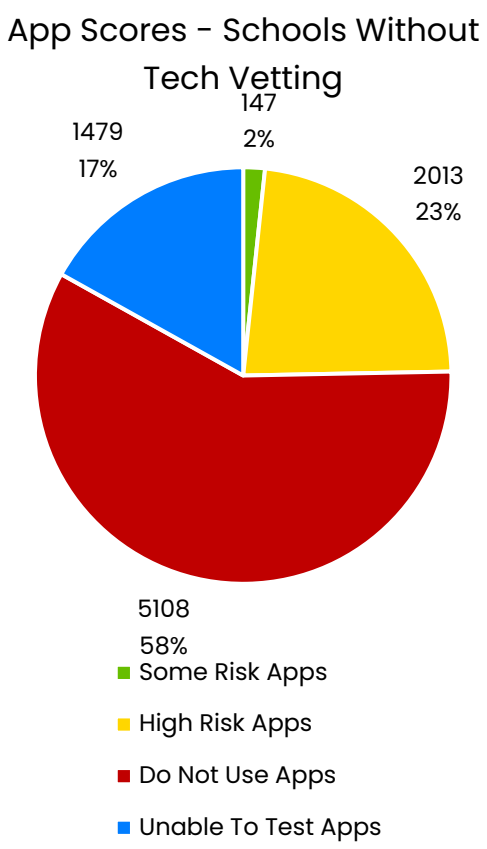


Figure 6.9

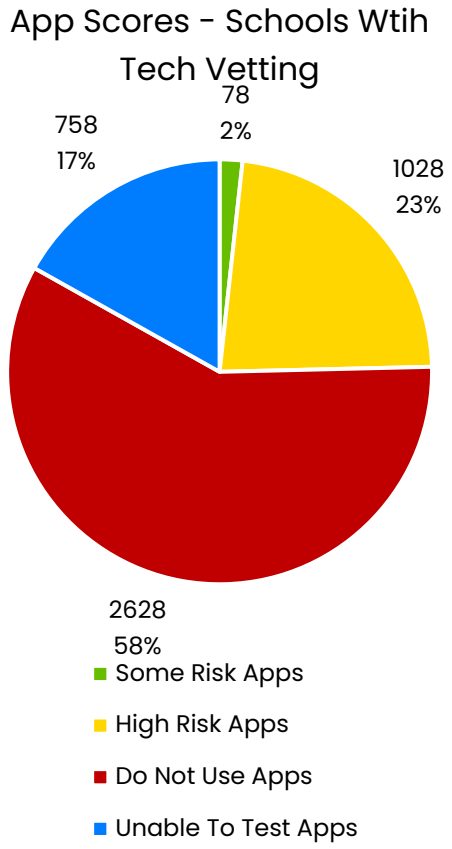


Figure 6.10

[15] Note that this proportion of scores is *not* comparable with the distribution of unique app scores shared in Findings Report 1. As can be seen, the total number of apps here is higher than the total number of apps tested, because many apps are used in multiple schools.

Another way to measure the impact of school vetting behaviors is to look at the *school composite score*, which is a weighted aggregate of all the apps recommended or required in the schools. The lower the school score, the safer the school's collection of apps. The average school score across the entire national dataset was 54.3. As can be seen in Figure 6.11 below, schools with no obvious vetting practices scored better as a group than any of the schools with obvious vetting practices.

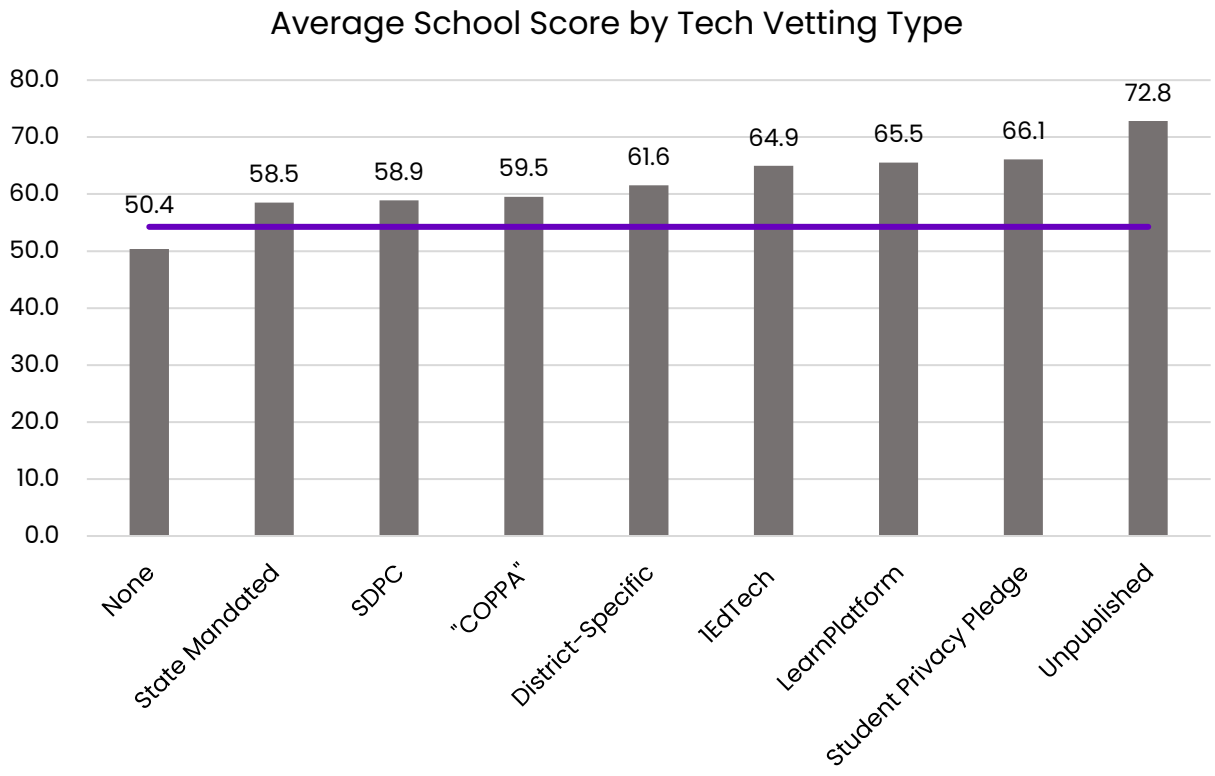


Figure 6.11

6.3.2.4 Advertising Behavior

We were also interested to see if school tech vetting had an obvious impact on the presence of apps with advertising (Figures 6.12 and 6.13). There is a meaningful reduction in the likelihood of ads in apps for schools with any kind of tech vetting (11.1% of apps compared to 16.1% of apps in schools without vetting, Figure 6.12). There is also a significant reduction in the likelihood of retargeting ads in apps for schools with any kind of tech vetting 2.1% compared to 7.0%, Figure 6.13).

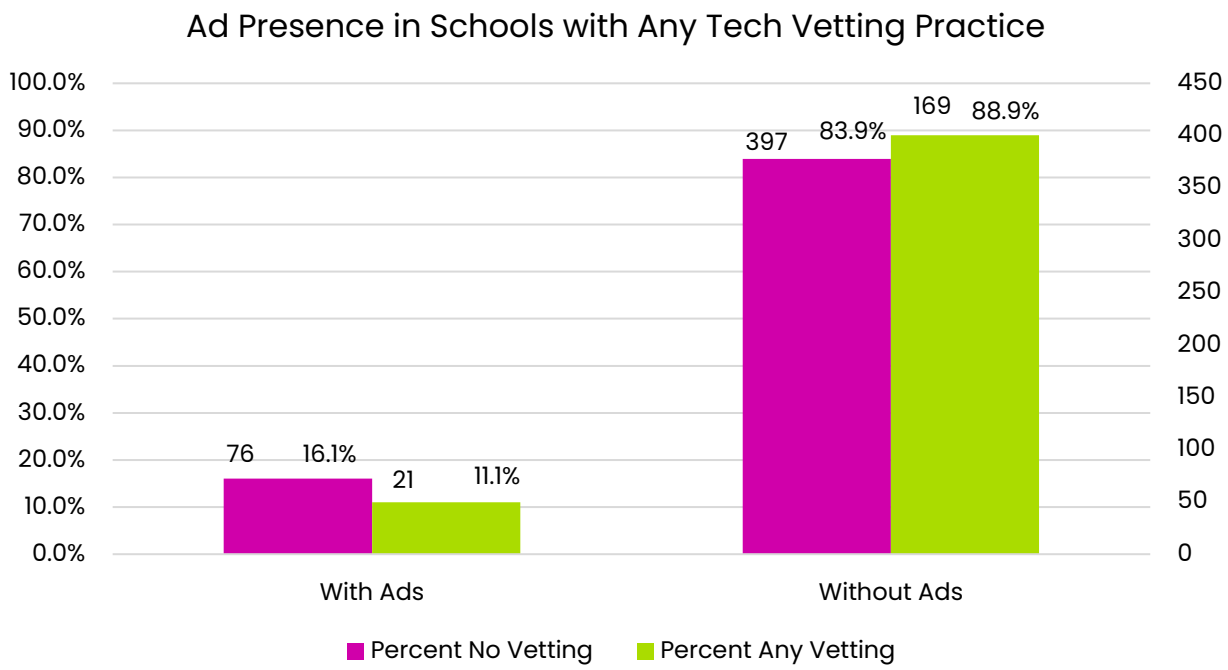


Figure 6.12

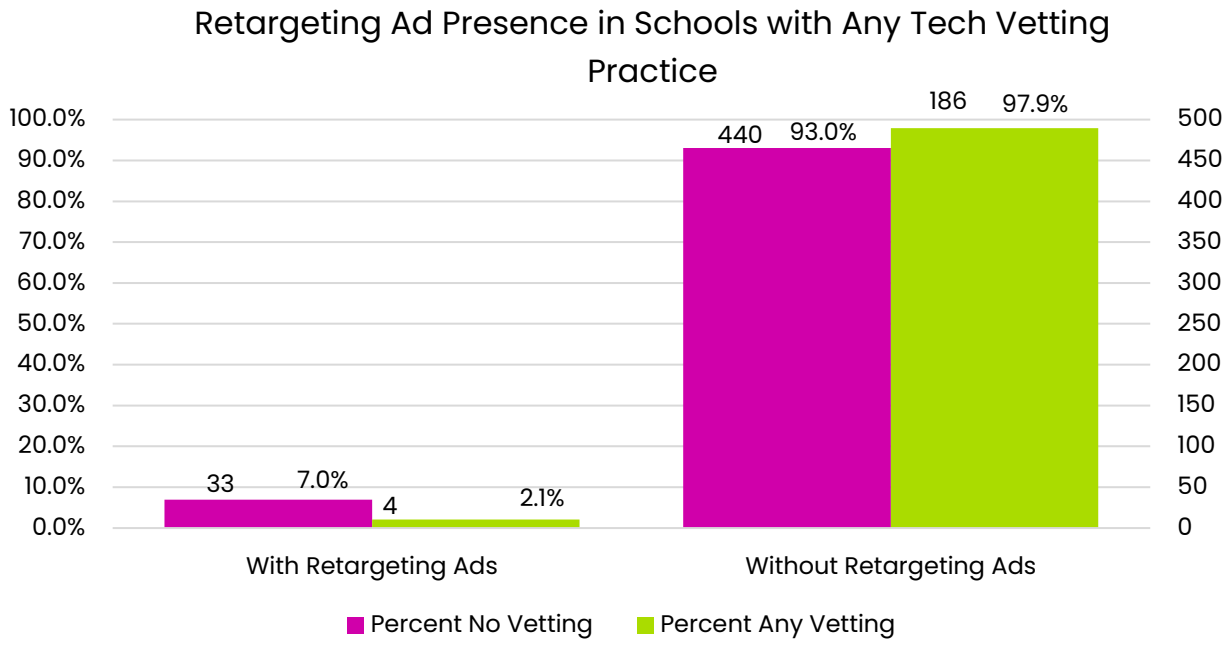


Figure 16.3

6.3.3 What to Make of the School Vetting Data

The data was not what we expected to see, and in fact, the trends were opposite of what we expected. What does this mean? There are several possibilities:

- Was our data collection flawed? Determining vetting simply by reviewing school and district websites likely didn't reflect the full reality of technology vetting being done by LEAs. Further research should be performed directly with LEAs to better understand the efficacy of various types of technology vetting.
- Could the very presence of systematic vetting policies and practices be giving schools a false sense of confidence in technology, resulting in the recommending of more technology?
- Is the ISL scoring rubric too strict?

In short, we suggest that deeper and more focused research in collaboration with LEAs is required to definitively determine vetting best practices.

6.4 SOPIPA Impacts on School Behaviors

As noted in Section 5, twenty-four states have student privacy laws along the lines of California's Student Online Personal Information Protection Act. We wondered how the states with SOPIPA-like regulations performed compared to states that didn't.[16]

As can be seen in figures 6.14a and 6.14b, schools in states with SOPIPA-like laws more frequently provided technology notice than schools in states without SOPIPA-like laws (48% of the schools versus 42% of the non-SOPIPA schools).

[16] Important to note that we measured only 13 schools in each state, resulting in 312 schools in states with SOPIPA-like laws, and 351 schools in states without. We suggest that a larger sample size be analyzed for confirmation.

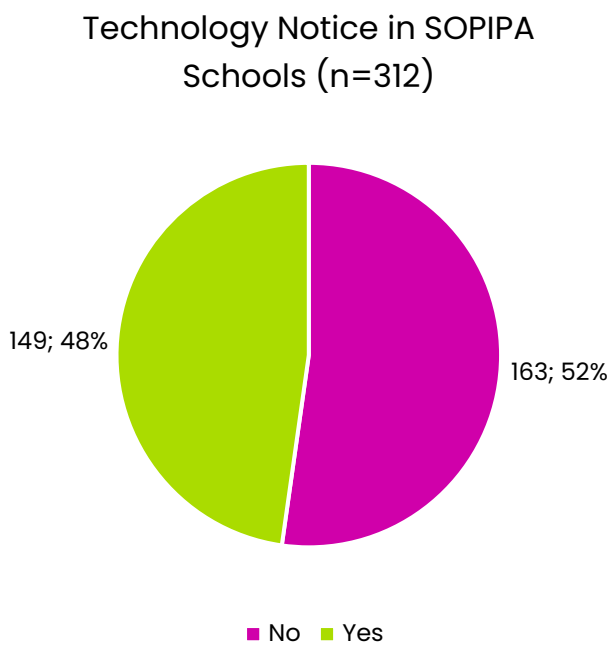


Figure 6.14a

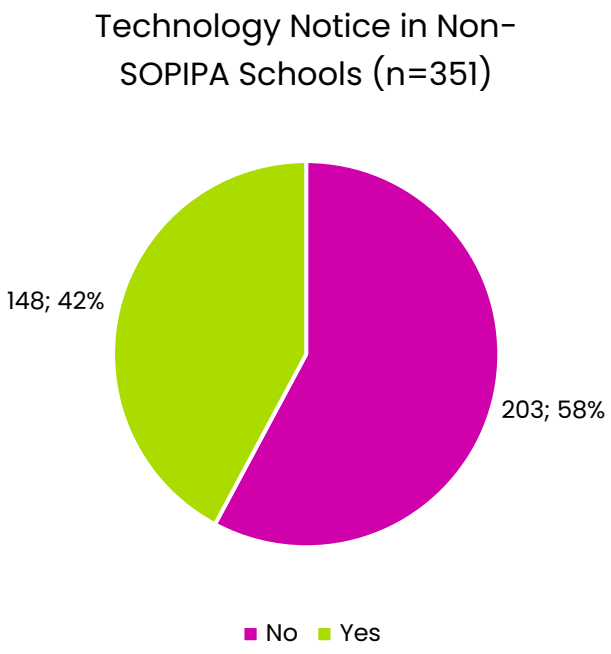


Figure 6.14b

Figure 6.15 shows technology consent behaviors in SOPIPA schools. The ability to consent to technology was virtually identical across the two groups: 14% of the SOPIPA schools offered some kind of consent versus 14.1% of schools in states without SOPIPA.

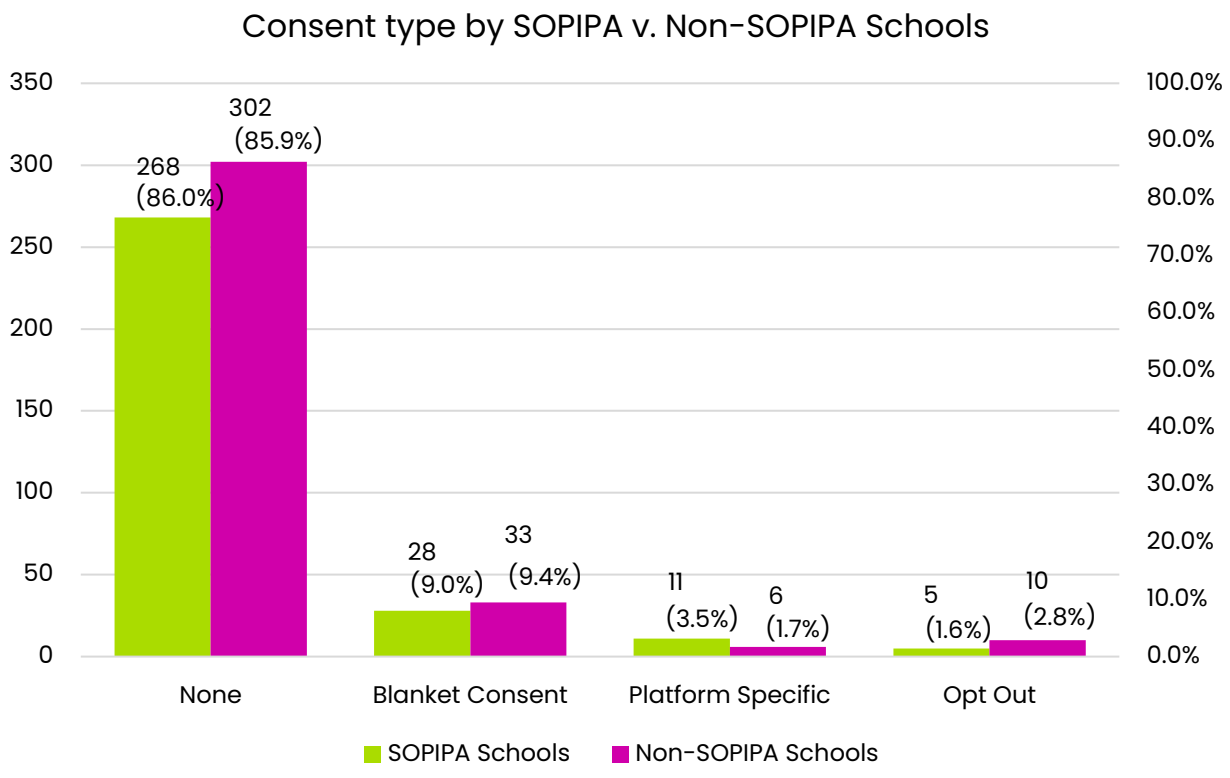


Figure 6.15

Figure 6.16 displays the scores of the apps used in schools with SOPIPA-like laws compared to the scores of the overall dataset. The apps in SOPIPA covered schools performed somewhat better with 58.1% of apps receiving a Do Not Use score, compared to 61.9% of the total dataset. There were significantly more High Risk apps (23.4% versus 13.9% in the overall sample), fewer Some Risk apps, and 5% fewer apps designated Unable to Test.

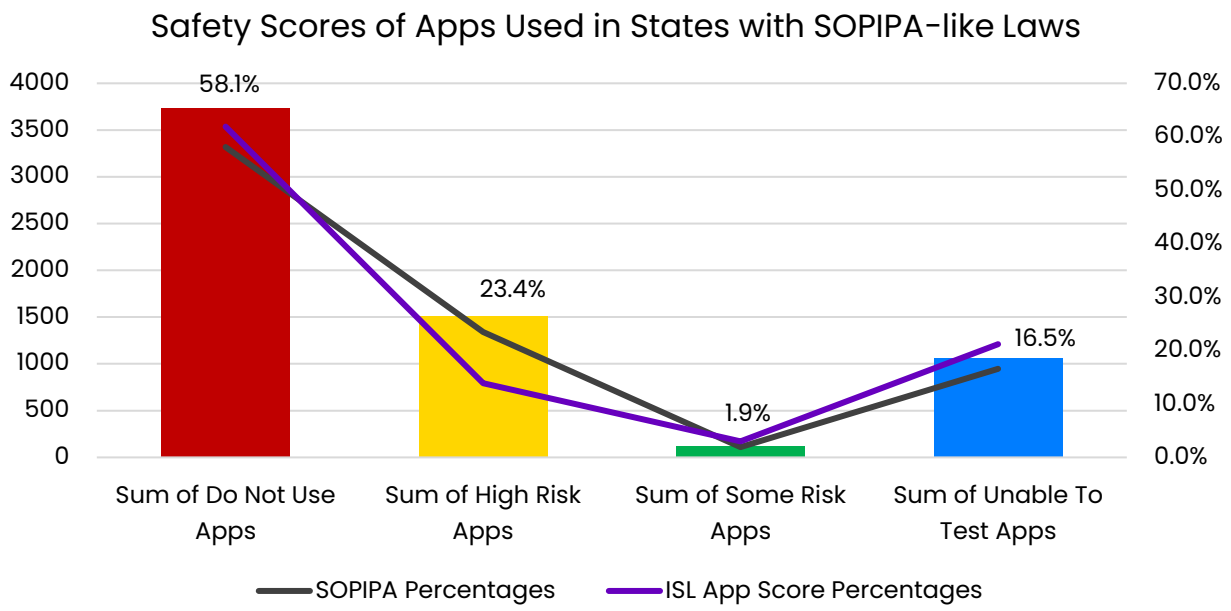


Figure 6.16

Figure 6.17 compares the average school composite score in states with and without SOPIPA-like laws. The average composite school score for the whole US was 54.3, and a lower score is better. From Figure 6.17, schools in states *without* SOPIPA-like laws did somewhat better than the national average, whereas schools in states *with* SOPIPA-like laws did somewhat worse. Like the earlier comparison of school composite scores, this could reflect over-confidence in tech vetting, resulting in the adoption of *more* apps—a higher number of technologies in use at a school will result in a higher school composite score.

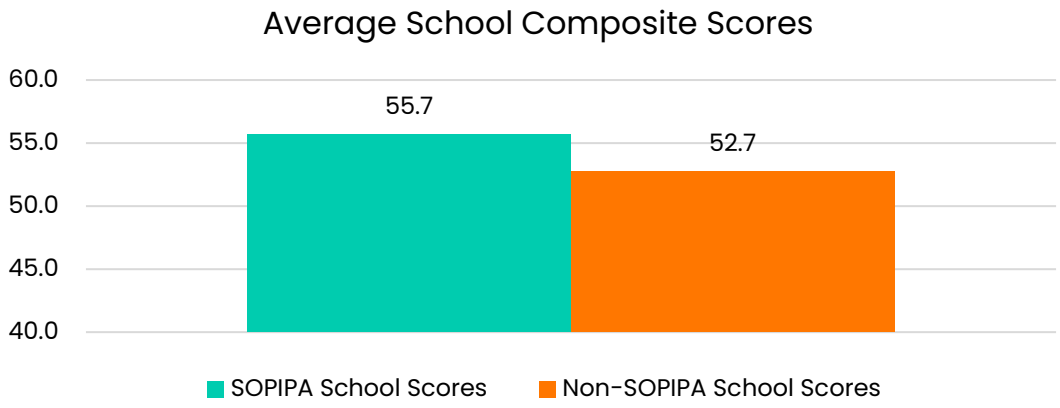


Figure 6.17

Finally, Figures 6.18 and 6.19 compare the presence of ads in apps in schools in states with and without SOPIPA-like laws. These charts indicate how many of the states in each group had EdTech apps with ads.

The set of states with SOPIPA-like laws were less likely to have ads in apps (54.2% compared to 69.2% of states without SOPIPA laws, Figure 6.18). 25.0% of the states with SOPIPA-like laws had apps with retargeting ads compared to 46.2% of states without (Figure 6.19). In other words, states without SOPIPA-like laws were nearly twice as likely (84.8% more likely) to have EdTech apps with retargeting ads. **Thus, it seems SOPIPA-like laws are reducing the likelihood of retargeting ads in EdTech apps in those states.**

However, another key takeaway here is that **25.0% of states with SOPIPA laws had schools using EdTech that had retargeting ads.** This is a disturbingly high percentage when coupled with the fact that our sample was relatively small, and the method of finding retargeting ads was somewhat opportunistic (as described in Findings Report 1). ISL believes it is likely that the actual percentage of SOPIPA law states with schools using EdTech with retargeting ads is significantly higher.

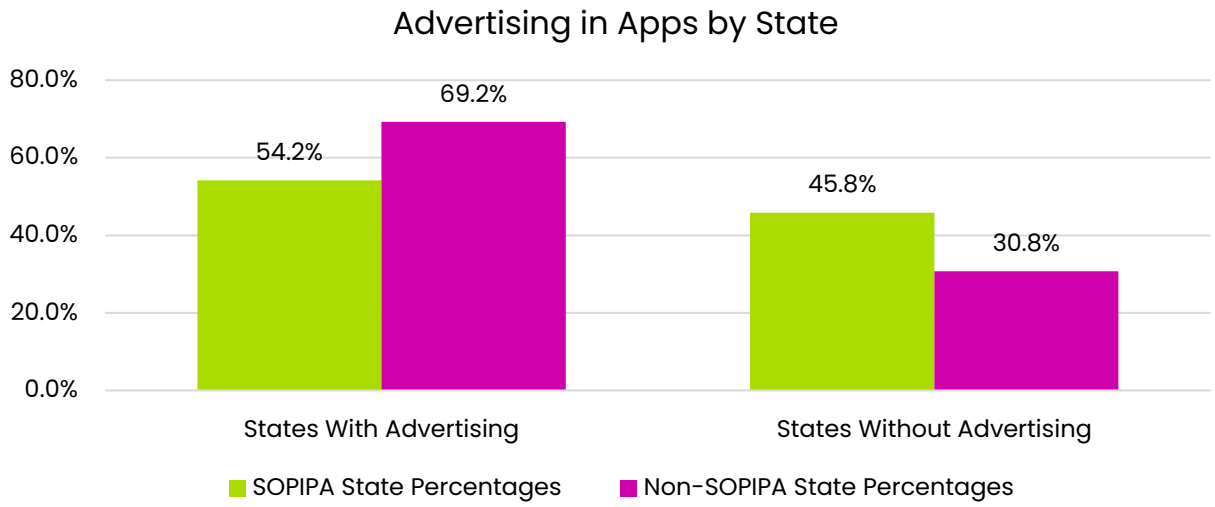


Figure 6.18

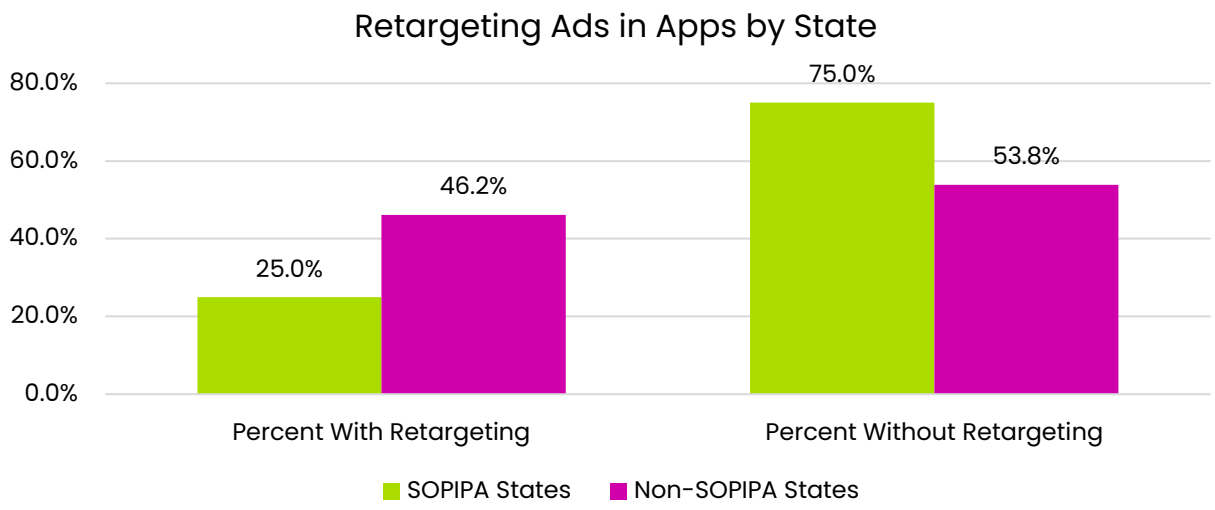


Figure 6.19

Figure 6.20 displays the presence of retargeting ads in apps in states with SOPIPA-like laws. The following states with SOPIPA laws **had apps with retargeting ads**: Arkansas, Colorado, Georgia, Illinois, Kansas, Maryland, Maine, Michigan, North Carolina, Nebraska, Tennessee, Texas, and Virginia.

The following states with SOPIPA laws **didn't have observed retargeting ads**: California, Connecticut, District of Columbia, Delaware, Hawaii, Iowa, New Hampshire, Nevada, Oregon, Utah, and Washington.

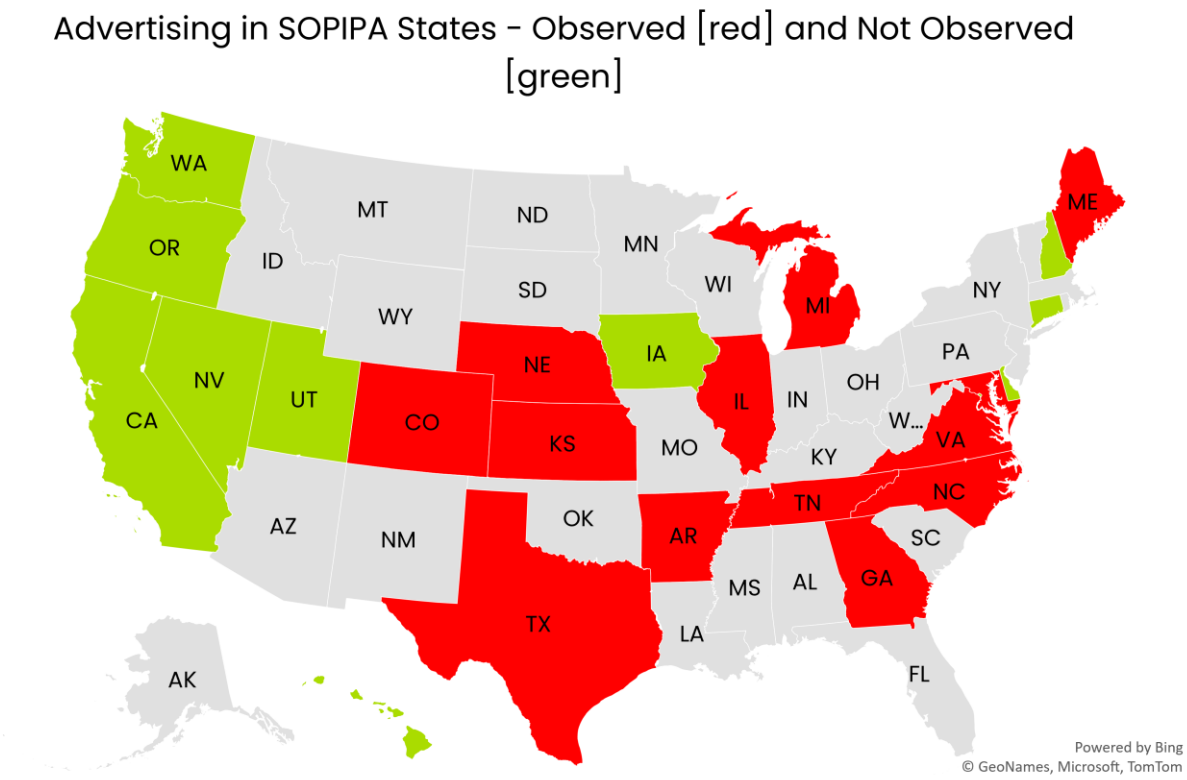


Figure 6.20

6.4.1 Are SOPIPA-like Laws Keeping Children Safer?

The information included in this section is included for completeness in describing the findings of the sampled data. It can't be considered as painting a complete and accurate picture, since we only tested technologies identified from 13 schools in each state.

Moreover, this research wasn't designed to test this question, so nothing here should be regarded as definitive. That said, from this limited dataset, it does appear that SOPIPA-like state laws may be helping to minimize the presence of ads and retargeting ads in EdTech apps. Though it's also quite possible that every state with SOPIPA-like laws has schools using EdTech apps with retargeting ads. Additional research is required.

7 App Analysis: Certification and "Promise" Efficacy

In this section, we shift from school behavior findings to app behaviors and the various types of external certifications and "promises" associated with the apps. "Promises" are either pledges (like the Student Privacy Pledge 2020) or other agreements app vendors make, such as Data Privacy Agreements facilitated by SDPC. In particular, we want to understand how apps with these certifications or promises behave relative to ISL safety findings. Our hypothesis is that apps with certifications or promises will be generally safer than the overall sample of apps.

The following certifications and promises are examined:

- COPPA Safe Harbor certifications
- Proprietary certifications (1EdTech)
- Student Privacy Pledge 2020 (promise)
- SDPC (promise)

It's important to note that the intentions of these certifications and promises differ from the ISL safety score, and this comparison isn't intended to be an evaluation of the efficacy of the methods. The comparison helps understand how the various methods may relate to each other.

There is a difference between the purpose and scope of certifications versus promises. For instance, the obligations of a COPPA Safe Harbor certification necessitate a thorough audit of app behaviors—likely beyond the extent of what ISL covered in the US K12 EdTech safety benchmark. The Student Privacy Pledge, however, is a commitment made by the vendor on behalf of both the company's and the apps' behaviors with respect to student data. SDPC provides a different kind of oversight, by providing boilerplate data privacy agreements that LEAs can execute with their technology vendors. Accordingly, in contrast to the certifications, the promises are mainly intended as deterrents and are ultimately enforceable if breached. Thus, promises don't necessarily require an evaluation of the product behavior (see table 7.1 below for a summary). Note that we did *not* confirm with the certifying entities if they did, in fact, audit the behavior of the software.

Table 7.1 Certification & Promise Types

Program/Promise	Purpose	Product Behavior Audit?	Enforceable?
COPPA Safe Harbor Programs	Ensure compliance with key aspects of COPPA regulation.	Yes	Yes
Proprietary Certifications	Ensure select product behaviors.	Yes	?
Student Privacy Pledge	Incentivize corporate and product safety behaviors through legally binding pledge.	No	Yes
SDPC	Incentivize corporate and product safety behaviors through legally binding agreements.	No	Yes
Vendor-Asserted COPPA Compliance	Communication from vendor asserting COPPA Compliance	No	Yes
ISL Safety Label	Quantify & publish product safety risks.	Yes	No

In total, 613 (35.8%) of apps in the sample had some kind of certification or promise. Figures 7.1.a shows the frequency of the various types of certifications and promises. Note that ISL counts and scores each version of an app individually, meaning the iOS version and the Android version of the same app count as two apps in our sample. As will be explained in section 7.1, due to their overwhelmingly unsafe performance, Community Engagement Platform (CEP) type apps distort the analysis so much that for most of section 7 we analyze the apps excluding CEP apps. Figure 7.1b shows the count of all certifications by type, excluding CEP apps.

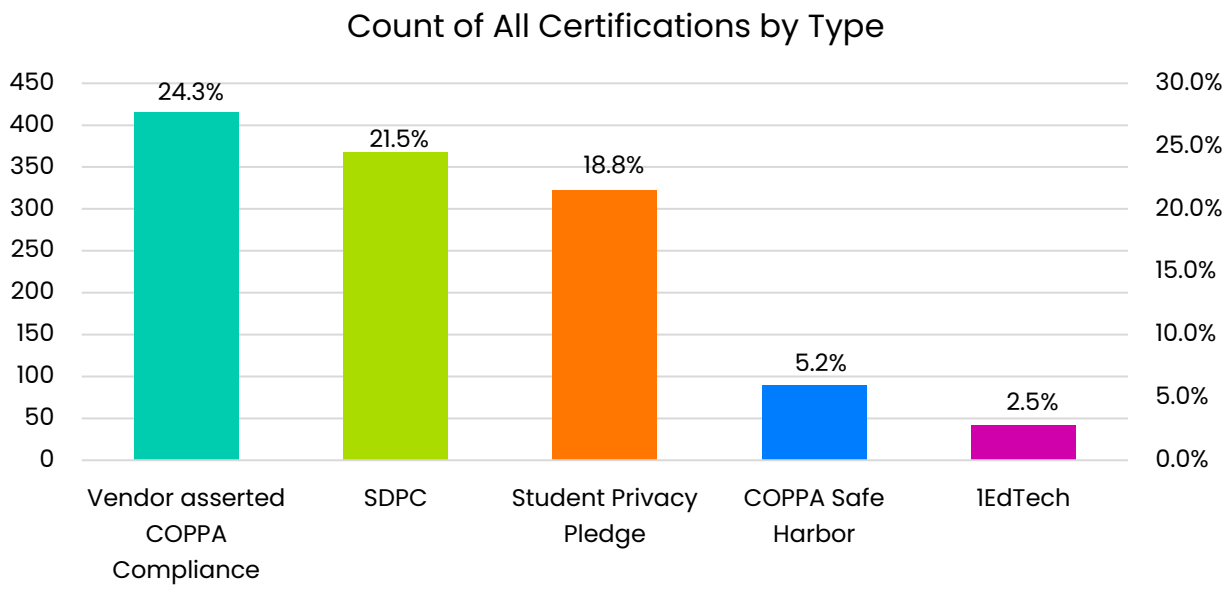


Figure 7.1a

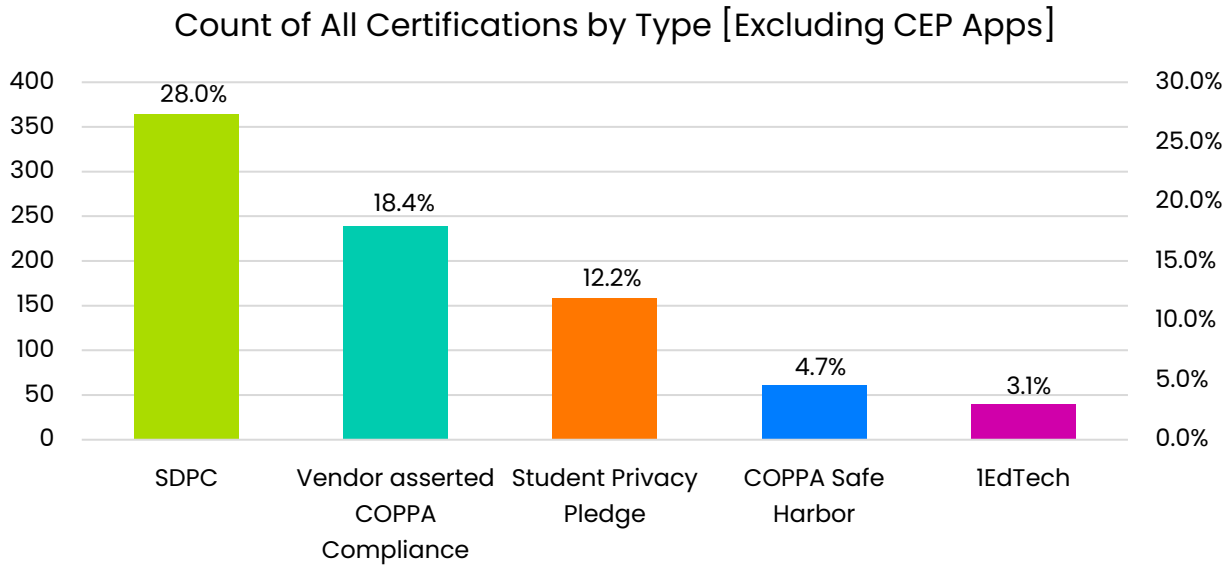


Figure 7.1b

Note that we analyze vendor-asserted COPPA compliance separately, but it is *not* an external certification or promise. We include it here for completeness; the sub-set of apps will be studied in section 7.4.

7.1 Overall Performance of Apps with Certifications/Promises

Table 7.2a summarizes the key safety findings, namely, the app safety scores and the presence of digital and retargeting advertising by certification or promise type.

Table 7.2a Summary of Key Safety Behaviors – All Apps

ALL APPS	# Apps	Do Not Use	High Risk	Some Risk	Unable to Test	Ads	Retar-geting Ads
ISL Benchmark	**1710**	**61.9%**	**14.0%**	**3.0%**	**21.2%**	**17.6%**	**9.7%**
Any Certification or Promise	613	64.1%	11.8%	2.1%	22.0%	15.7%	7.9%
No Certifications or Prom-ises	1097	60.6%	15.2%	3.5%	20.7%	18.6%	10.7%
CERTIFICATIONS							
All Certifications	111	63.1%	11.7%	0.0%	25.2%	20.5%	0.0%
ALL COPPA Safe Harbor Cer-tifications	77	71.4%	13.0%	0.0%	15.6%	26.2%	0.0%
iKeepSafe	40	72.5%	10.0%	0.0%	17.5%	24.2%	0.0%
KidSafe	25	72.0%	16.0%	0.0%	12.0%	18.0%	0.0%
Privo	10	75.0%	25.0%	0.0%	25.0%	40.0%	0.0%
Proprietary							
1EdTech	42	40.5%	11.9	0.0%	47.6%	0.0%	0.0%
PROMISES							
Student Privacy Pledge	321	68.9%	9.6%	1.9%	19.6%	18.1%	13.1%
SDPC	368	53.5%	16.0%	1.9%	28.5%	8.0%	2.3%
SELF-ASSERTED COPPA COM-PLIANCE							
Self-Asserted COPPA Com-pliance Only	415	75.7%	10.4%	1.0%	13.0%	13.9%	6.4%

* Note that the percentage of ads and retargeting ads reflects a total volume of 1348 apps.

These findings were surprising. Through a suggestion from the Future of Privacy Forum, we decided to filter out the Community Engagement Platform apps (aka "school utility apps"). As noted in Findings Report 1, these apps had more safety

concerns than other EdTech categories of apps.[17] Tables 7.2b and 7.2c show the safety risks of CEP apps compared to non-CEP apps. As can be seen (Table 7.2b), the CEP apps in the certified or promising apps clearly distort the findings. As shown in Table 7.2c, when we remove the CEP apps from the analysis, apps with any kind of certification or promise have fewer Do Not Use scores, and significantly fewer ads and retargeting ads than apps with no certification or promise.

Table 7.2b – Summary of Key Safety Behaviors – CEP Apps Only

ALL CEP APPS	# Apps	Do Not Use	High Risk	Some Risk	Unable to Test	Ads	Retargeting Ads
ISL Benchmark	**412**	**85.0%**	**10.4%**	**0.2%**	**4.4%**	**23.4%**	**11.7%**
Any Certification or Promise	182	94.0%	2.8%	0.0%	3.3%	29.0%	18.2%
No Certifications or Promises	230	77.8%	16.5%	0.4%	5.2%	18.8%	6.4%
CERTIFICATIONS							
All Certifications	18	61.1%	22.2%	0.0%	16.7%	40.0%	0.0%
ALL COPPA Safe Harbor Certifications	16	62.5%	25.0%	0.0%	12.5%	42.9%	0.0%
iKeepSafe	16	62.5%	25.0%	0.0%	12.5%	42.9%	0.0%
KidSafe	0	--	--	--	--	--	--
Privo	0	--	--	--	--	--	--
Proprietary							
1EdTech	2	50.0%	0.0%	0.0%	50.0%	0.0%	0.0%
PROMISES							
Student Privacy Pledge	163	98.2%	0.6%	0.0%	1.2%	27.8%	19.8%
SDPC	4	25.0%	0.0%	0.0%	75.0%	0.0%	0.0%
SELF-ASSERTED COPPA COMPLIANCE							
Self-Asserted COPPA Compliance Only	176	80.1%	15.3%	0.6%	4.0%	18.3%	6.5%

[17] CEP apps will be further analyzed in a future publication.

Table 7.2c – Summary of Key Safety Behaviors—All Apps, Excluding CEP Apps

ALL NON-CEP APPS	# Apps	Do Not Use	High Risk	Some Risk	Unable to Test	Ads	Retar-geting Ads
ISL Benchmark	**1298**	**54.6%**	**15.1%**	**3.9%**	**26.5%**	**15.2%**	**8.9%**
Any Certification or Promise	431	51.5%	15.6%	3.0%	29.9%	7.9%	2.0%
No Certifications or Prom-ises	867	56.1%	14.9%	4.3%	24.8%	18.6%	12.1%
CERTIFICATIONS							
All Certifications	93	63.4%	9.7%	0.0%	26.9%	16.2%	0.0%
ALL COPPA Safe Harbor Cer-tifications	61	73.8%	9.8%	0.0%	16.4%	21.6%	0.0%
iKeepSafe	24	79.2%	0.0%	0.0%	20.8%	10.5%	0.0%
KidSafe	25	72.0%	16.0%	0.0%	12.0%	18.2%	0.0%
Privo	10	60.0%	20.0%	0.0%	20.0%	50.0%	0.0%
Proprietary							
1EdTech	40	5	12.5%	0.0%	47.5%	0.0%	0.0%
PROMISES							
Student Privacy Pledge	158	38.6%	19.0%	3.8%	38.6%	2.1%	2.1%
SDPC	364	53.9%	16.2%	1.9%	28.2%	8.0%	2.3%
SELF-ASSERTED COPPA COM-PLIANCE							
Self-Asserted COPPA Com-pliance Only	239	55.7%	13.8%	1.7%	28.9%	11.2%	7.1%

7.1.1 Key Safety Findings – Excluding CEP Apps

In the set of all apps excluding CEP apps, 431 apps (33.2%) had some kind of certification or promise.

1. While addressed in Findings Report 1, it's worth reiterating that **School Utility apps (part of the CEP category) are problematic and should not be used by students (or parents).** Appendix B lists all the CEP apps in the benchmark. If you're a student or parent using a school or district branded app for school info, it's likely to be one of these unsafe CEP apps.

    a. ISL also recommends that certification and promising organizations screen for these kinds of apps, given the data sharing risks.
2. The set of apps with certifications or promises are safer than the set of apps without certifications or promises, and safer than the overall set of non-CEP apps.
    - Apps without certifications or promises were 8.9% more likely to have a DNU score than certified/promising apps.
    - Apps without certifications or promises were 1.34 times as likely to have digital ads and 5 times as likely to have retargeting ads than certified/promising ads.
3. Apps with certifications had fewer retargeting ads COPPA Safe Harbor certifications (iKeepSafe, KidSafe, and Privo) were excellent with respect to retargeting ads, but worse than uncertified apps in terms of Do Not Use scores and presence of digital advertising.
    - No retargeting ads were found in any of the COPPA Safe Harbor certified apps.
    - Digital ads were proportionally higher in Kidsafe and iKeepSafe certified apps than in uncertified apps and the total data set.
        - NOTE that this could be a side-effect from our testing methodology, which covered only the free and publicly available versions of the apps, which are typically ad-supported. However, given that these are EdTech apps for K-12 students, we remain firm that they should contain no advertising while the current adtech realtime bidding algorithms and infrastructures are in place.
    - COPPA Safe Harbor certified apps had a higher percent of Do Not Use scores than uncertified/promising apps as well as the overall data set.
4. While we only tested about 50% of the apps (20 in total; 10 unique apps), 1EdTech's proprietary certification resulted in the safest behaviors of all certified/promising apps:
    - A relatively low percent of Do Not Use apps (40%),
    - No digital ads and no retargeting ads.
5. Both promises (Student Privacy Pledge and SDPC) resulted in fewer Do Not Use scores than uncertified/promising apps, and the overall sample.

- Student Privacy Pledge had the fewest number of Do Not Use apps of all studied subsets, at 38.6%.
- However, both promises had a small presence of retargeting ads, 2.1% and 2.3% respectively.

6. **Certifications** seem to be **more effective** than **promises** at eliminating **re-targeting ads** (Table 7.2c).
7. Apps with **promises** have **better safety scores** than the **certified apps**.
8. Apps with self-asserted COPPA compliance performed better than the overall sample and apps with no certifications or promises.
    - "Self-asserted COPPA compliance" means that the vendor publicly stated that the app/service was COPPA compliant *and* there was no third-party certification. Such an assertion was typically noted in the app's privacy policy.
        - These apps are included in the "No Certifications or Promises" count but were also examined as a subset of apps.
    - Going into the benchmark, we expected vendor-asserted COPPA compliance to be ineffectual, but **self-asserted COPPA compliance appears to be somewhat meaningful, resulting in somewhat safer apps** than uncertified and the overall sample set.
    - With retargeting ads at 7.1%, vendor-asserted COPPA compliant apps had the highest percent of retargeting ads observed of all the examined subsets of apps, which was still somewhat better than the overall sample (8.9%) and apps with no certifications or promises (12.1%).

7.1.2 Do Not Use Scores in Certified/Promising Apps

Figures 7.2a and 7.2b (below) compare the safety scores of apps that have been certified or have a privacy promise against the average scores of the overall data set. As can be seen in Figure 7.2b, removing the CEP apps results in fewer DNU scores but more untested apps.

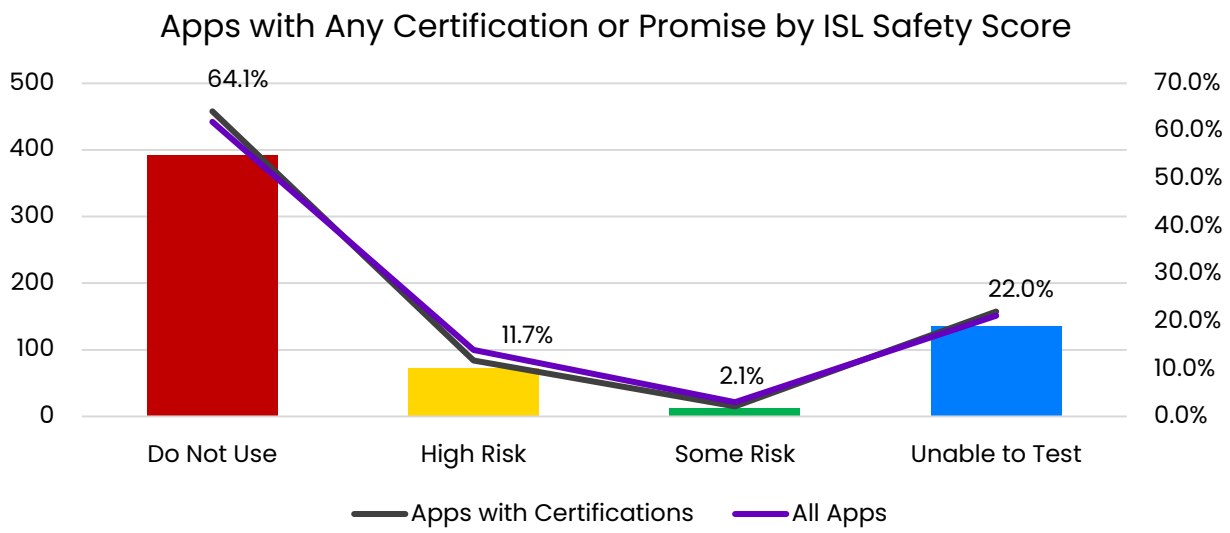


Figure 7.2a

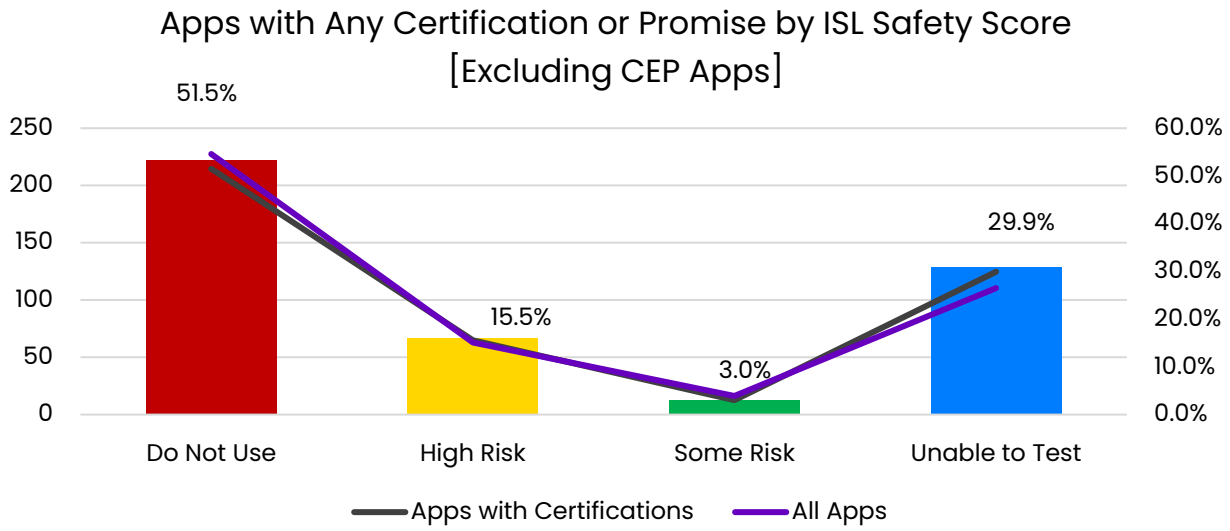


Figure 7.2b

Tables 7.3a and 7.3b below display the Do Not Use triggers found in all apps and all apps excluding CEP apps, respectively. We can see that the exclusion of CEP apps results in fewer DNU triggers due to Amazon network traffic (from 27.1% of DNU apps to 23.2%), Facebook network traffic (from 44.9% of DNU apps to 41.7%), and Twitter network traffic (from 18.7% to 12.3%).

Interestingly, we see a slight increase in the percent in each, Adobe, Amazon, Facebook, and data broker SDK triggers. As expected, the removal of CEP apps from the sample eliminated all the MaxPreps DNU triggers, as MaxPreps was only found in the CEP apps.

Table 7.3a Do Not Use Triggers in All Apps

	# Do Not Use Apps	Adobe Network Traffic	Amazon Network Traffic	Facebook Network Traffic	Twitter Network Traffic	SDKs Owned by Adobe	SDKs Owned by Amazon	SDKs Owned by Facebook	SDKs Owned by Twitter	SDKs Owned by Data Brokers	Ads	Permissions	MaxPreps
ISL Benchmark	**1059**	**2.2%**	**27.1%**	**44.9%**	**18.7%**	**2.6%**	**5.3%**	**52.7%**	**5.9%**	**2.8%**	**22.4%**	**3.0%**	**3.2%**
Any Certification or Promise	**393**	**2.8%**	**26.0%**	**49.1%**	**24.2%**	**1.8%**	**4.3%**	**58.0%**	**7.1%**	**2.5%**	**19.1%**	**4.1%**	**7.6%**
No Certifications or Promises	**663**	**1.8%**	**27.1%**	**42.4%**	**15.5%**	**3.2%**	**5.3%**	**49.6%**	**5.1%**	**3.0%**	**24.4%**	**2.4%**	**0.6%**
CERTIFICATIONS													
All Certifications	**70**	**0.0%**	**25.7%**	**38.6%**	**18.6%**	**1.4%**	**0.0%**	**45.7%**	**0.0%**	**2.9%**	**24.3%**	**0.0%**	**0.0%**
ALL COPPA Safe Harbor Certifications	**55**	**0.0%**	**18.6%**	**39.0%**	**18.6%**	**1.7%**	**0.0%**	**44.1%**	**0.0%**	**3.4%**	**28.8%**	**0.0%**	**0.0%**
iKeepSafe	**29**	**0.0%**	**10.3%**	**31.0%**	**24.1%**	**0.0%**	**0.0%**	**37.9%**	**0.0%**	**6.9%**	**27.6%**	**0.0%**	**0.0%**
KidSafe	**18**	**0.0%**	**33.3%**	**50.0%**	**22.2%**	**5.6%**	**0.0%**	**50.0%**	**0.0%**	**0.0%**	**22.2%**	**0.0%**	**0.0%**
Privo	**6**	**0.0%**	**33.3%**	**50.0%**	**0.0%**	**0.0%**	**0.0%**	**66.7%**	**0.0%**	**0.0%**	**66.7%**	**0.0%**	**0.0%**
Proprietary													
1EdTech	**17**	**0.0%**	**23.5%**	**41.2%**	**11.8%**	**0.0%**	**0.0%**	**47.1%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**
PROMISES													
Student Privacy Pledge	**222**	**1.8%**	**29.1%**	**54.3%**	**32.7%**	**0.9%**	**3.1%**	**61.9%**	**10.3%**	**0.9%**	**21.1%**	**6.7%**	**13.5%**
SDPC	**197**	**3.6%**	**24.9%**	**39.6%**	**7.6%**	**2.0%**	**7.6%**	**54.8%**	**2.5%**	**5.1%**	**3.0%**	**0.5%**	**0.0%**
SELF-ASSERTED COPPA COMPLIANCE													
Only Vendor Self Asserted COPPA Compliance	**314**	**2.2%**	**33.8%**	**34.1%**	**12.4%**	**1.6%**	**2.9%**	**38.5%**	**0.6%**	**1.9%**	**15.9%**	**0.6%**	**0.6%**

Table 7.3b Do Not Use Triggers in All Non-CEP Apps

ALL NON-CEP APPS	# Do Not Use Apps	Adobe Network Traffic	Amazon Network Traffic	Facebook Network Traffic	Twitter Network Traffic	SDKs Owned by Adobe	SDKs Owned by Amazon	SDKs Owned by Facebook	SDKs Owned by Twitter	SDKs Owned by Data Brokers	Advertising	Permissions	Max-Preps
ISL Benchmark	**708**	**2.5%**	**23.2%**	**41.7%**	**12.3%**	**3.5%**	**7.9%**	**53.0%**	**4.5%**	**4.2%**	**20.5%**	**2.3%**	**0.0%**
Any Certification or Promise	**222**	**3.2%**	**25.2%**	**39.6%**	**8.6%**	**2.3%**	**7.7%**	**52.7%**	**2.3%**	**4.5%**	**10.8%**	**1.4%**	**0.0%**
No Certifications or Promises	**486**	**2.3%**	**22.2%**	**42.6%**	**14.0%**	**4.1%**	**8.0%**	**53.1%**	**5.6%**	**4.1%**	**24.9%**	**2.7%**	**0.0%**
CERTIFICATIONS													
All Certifications	**59**	**0.0%**	**27.1%**	**37.3%**	**11.9%**	**1.7%**	**0.0%**	**54.2%**	**0.0%**	**3.4%**	**18.6%**	**0.0%**	**0.0%**
ALL COPPA Safe Harbor Certifications	**45**	**0.0%**	**20.0%**	**42.2%**	**11.1%**	**2.2%**	**0.0%**	**57.8%**	**0.0%**	**4.4%**	**24.4%**	**0.0%**	**0.0%**
iKeepSafe	**19**	**0.0%**	**5.3%**	**26.3%**	**5.3%**	**0.0%**	**0.0%**	**57.9%**	**0.0%**	**10.5%**	**10.5%**	**0.0%**	**0.0%**
KidSafe	**18**	**0.0%**	**33.3%**	**50.0%**	**22.2%**	**5.6%**	**0.0%**	**50.0%**	**0.0%**	**0.0%**	**22.2%**	**0.0%**	**0.0%**
Privo	**6**	**0.0%**	**33.3%**	**50.0%**	**0.0%**	**0.0%**	**0.0%**	**66.7%**	**0.0%**	**0.0%**	**66.7%**	**0.0%**	**0.0%**
Proprietary													
1EdTech	**16**	**0.0%**	**43.8%**	**18.8%**	**12.5%**	**0.0%**	**0.0%**	**50.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**
PROMISES													
Student Privacy Pledge	**61**	**0.0%**	**34.4%**	**32.8%**	**4.9%**	**0.0%**	**11.5%**	**44.3%**	**0.0%**	**3.3%**	**3.3%**	**3.3%**	**0.0%**
SDPC	**196**	**3.6%**	**25.0%**	**39.3%**	**7.7%**	**2.0%**	**7.7%**	**55.1%**	**2.6%**	**5.1%**	**10.7%**	**0.5%**	**0.0%**
SELF-ASSERTED COPPA COMPLIANCE													
Only Vendor Self Asserted COPPA Compliance	**133**	**4.5%**	**30.8%**	**33.1%**	**9.8%**	**3.8%**	**6.8%**	**48.1%**	**0.8%**	**4.5%**	**14.3%**	**1.5%**	**0.0%**

Tables 7.4a and 7.4b display the number of Do Not Use criteria found in all the DNU apps in the total sample and all DNU apps in the non-CEP apps. Note that removing the CEP apps from the sample reduces the frequency of multiple DNU criteria. In the set of all apps only 38.7% of the DNU apps had only one criterion. Removing the CEP apps from the set increases the percentage of DNU apps with only one criterion to 57.2%. The chart shows this in a reddish color since it's higher than the total sample set percentage of 48.0%, but this should be considered a positive difference. We want to see fewer DNU triggers in the apps.

Even though the certified apps had higher rates of Do Not Use apps, table 7.4b clearly shows that for most of the certifications and promises, most of the Do Not Use apps had only one criterion.

KidSafe and Privo COPPA Safe Harbor certified apps (albeit a very small sample) were both more likely to result in multiple Do Not Use criteria.

Table 7.4a Number of Do Not Use Criteria in All Apps

ALL APPS	# Do Not Use Apps	1 DNU Criterion	2 DNU Criteria	3 DNU Criteria	4 DNU Criteria	5 DNU Criteria	6 DNU Criteria
ISL Benchmark	**1059**	**42.3%**	**33.2%**	**17.8%**	**4.8%**	**1.5%**	**0.3%**
Any Certification or Promise	393	38.7%	29.3%	22.4%	6.6%	2.5%	0.5%
No Certifications or Promises	665	44.4%	35.6%	17.8%	4.8%	1.5%	0.3%
CERTIFICATIONS							
All Certifications	70	58.6%	25.7%	15.7%	0.0%	0.0%	0.0%
ALL COPPA Safe Harbor Certifications	55	52.7%	29.1%	18.2%	0.0%	0.0%	0.0%
iKeepSafe	29	69.0%	24.1%	6.9%	0.0%	0.0%	0.0%
KidSafe	18	39.0%	39.0%	22.0%	0.0%	0.0%	0.0%
Privo	6	33.3%	16.7%	50.0%	0.0%	0.0%	0.0%
Proprietary							
1EdTech	17	63.6%	9.1%	4.5%	0.0%	0.0%	0.0%
Promises							
Student Privacy Pledge	222	27.8%	27.4%	29.1%	10.8%	3.6%	0.9%
SDPC	197	57.1%	30.3%	10.6%	1.0%	1.0%	0.0%
SELF-ASSERTED COPPA COMPLIANCE							
Only Vendor Self Asserted COPPA Compliance	314	44.3%	29.6%	12.1%	1.0%	0.3%	0.0%

Table 7.4b Number of Do Not Use Criteria in Non-CEP Apps

ALL NON-CEP APPS	# Do Not Use Apps	1 DNU Criterion	2 DNU Criteria	3 DNU Criteria	4 DNU Criteria	5 DNU Criteria	6 DNU Criteria
ISL Benchmark	**708**	**48.0%**	**34.5%**	**12.9%**	**3.4%**	**1.1%**	**0.1%**
Any Certification or Promise	222	57.2%	30.2%	10.8%	0.9%	0.9%	0.0%
No Certifications or Promises	486	43.8%	36.4%	13.8%	4.5%	1.2%	0.2%
CERTIFICATIONS							
All Certifications	59	61.0%	23.7%	15.3%	0.0%	0.0%	0.0%
ALL COPPA Safe Harbor Certifications	45	55.6%	26.7%	17.8%	0.0%	0.0%	0.0%
iKeepSafe	19	84.2%	15.8%	0.0%	0.0%	0.0%	0.0%
KidSafe	18	38.9%	38.9%	22.2%	0.0%	0.0%	0.0%
Privo	6	33.3%	16.7%	50.0%	0.0%	0.0%	0.0%
Proprietary	16	81.3%	12.5%	6.3%	0.0%	0.0%	0.0%
1EdTech	16	81.3%	12.5%	6.3%	0.0%	0.0%	0.0%
Promises							
Student Privacy Pledge	61	67.2%	27.9%	4.9%	0.0%	0.0%	0.0%
SDPC	196	56.6%	30.6%	10.7%	1.0%	1.0%	0.0%
VENDOR SELF-ASSERTED COPPA							
Only Vendor Self Asserted COPPA Compliance	133	55.6%	33.1%	9.8%	0.8%	0.8%	0.0%

7.1.3 Advertising in Certified/Promising Apps

In addition to comparing the app scores, we were also interested in understanding how the certified/promising apps performed with respect to advertising (Figures 7.3a and 7.3b). Once again, removing the CEP apps from the sample (Figure 7.3b) improves the results with only 2.0% of apps with any kind of certification or promise having retargeting ads compared to 12.8% of the overall data set. Similarly, only 7.9% of apps with certifications or promises had digital ads compared

to 19.7% of the total sample. The certifications and promises appear to be having a positive effect on reducing the amount of advertising and retargeting ads in the EdTech apps.

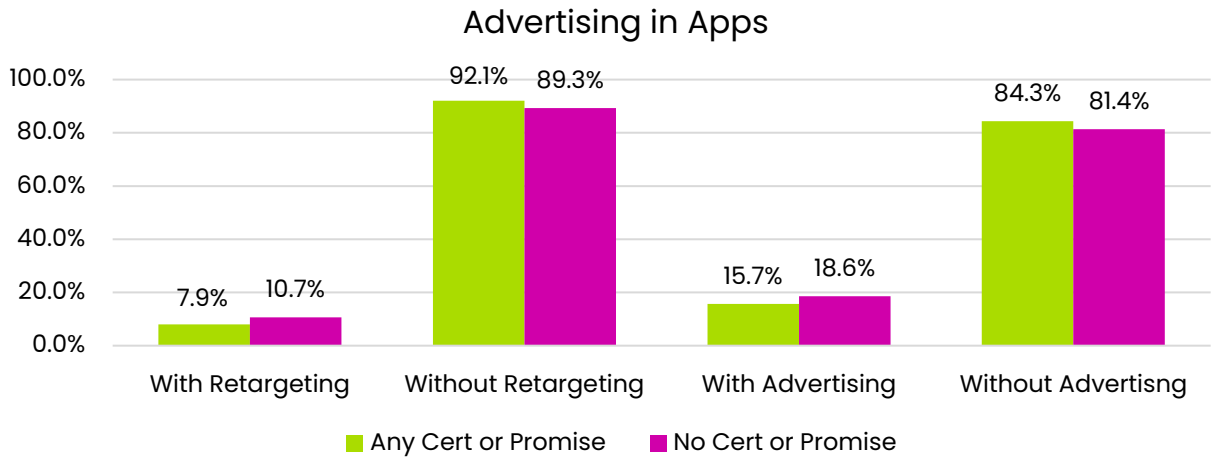


Figure 7.3a

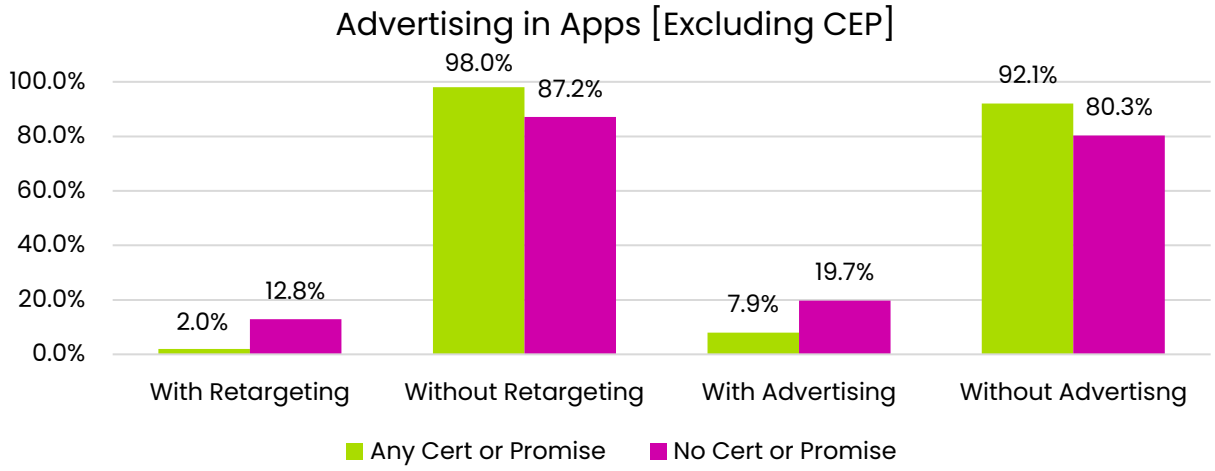


Figure 7.3b

Figures 7.4a and 7.4b show the number and percent of apps containing ads by certification or promise type. Focusing on Figure 7.4b, the removal of CEP apps results in the two promises and the proprietary 1EdTech certification having a lower percentage of apps with ads than the benchmark average. COPPA Safe

Harbor apps however have a higher percentage (21.6% of the COPPA Safe Harbor certified apps) than the benchmark average (15.2%).

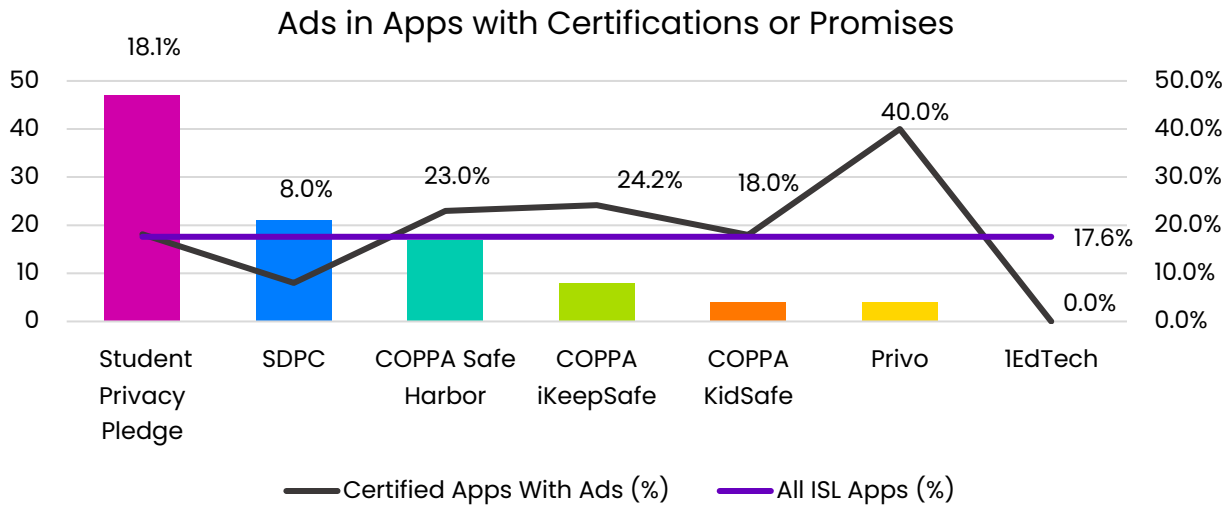


Figure 7.4a

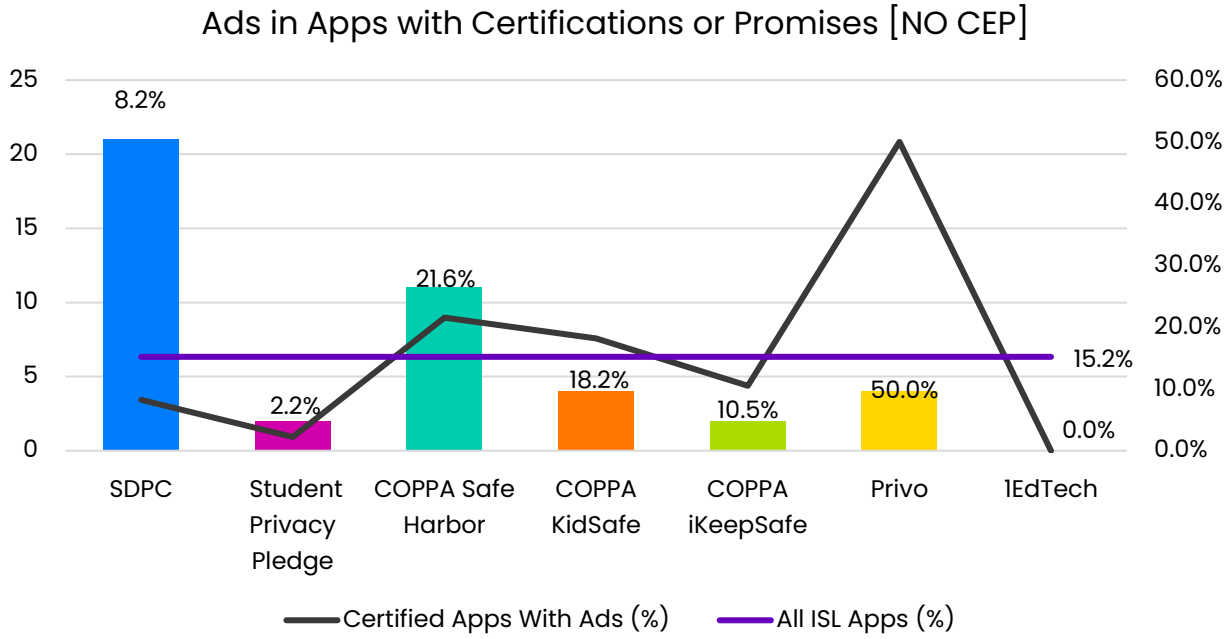


Figure 7.4b

Figures 7.5a and 7..b show the number and percentage of apps containing retargeting ads by certification or promise type. Again, focusing on Figure 7.5b, all of the certifications and promises result in fewer retargeting ads, with all the certifications (COPPA Safe Harbor plus the 1EdTech certification) resulting in no retargeting ads. The SDPC and Student Privacy Pledge promising apps had only 2.4% and 2.2% of the apps with retargeting ads. This could be attributed to the fact that the promises don't typically entail an evaluation of the app behavior.

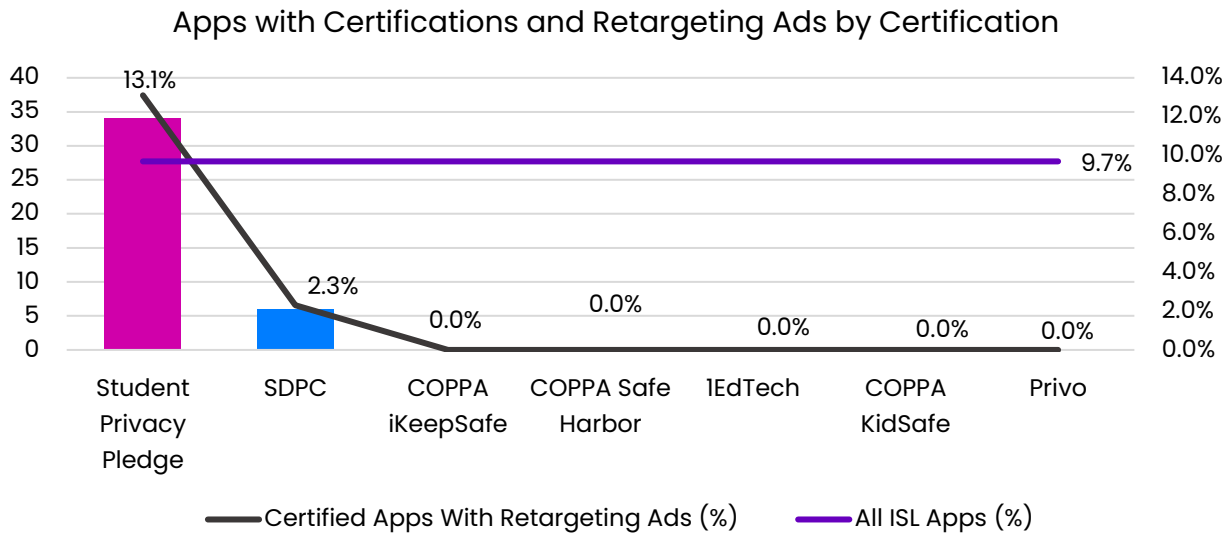


Figure 7.5a

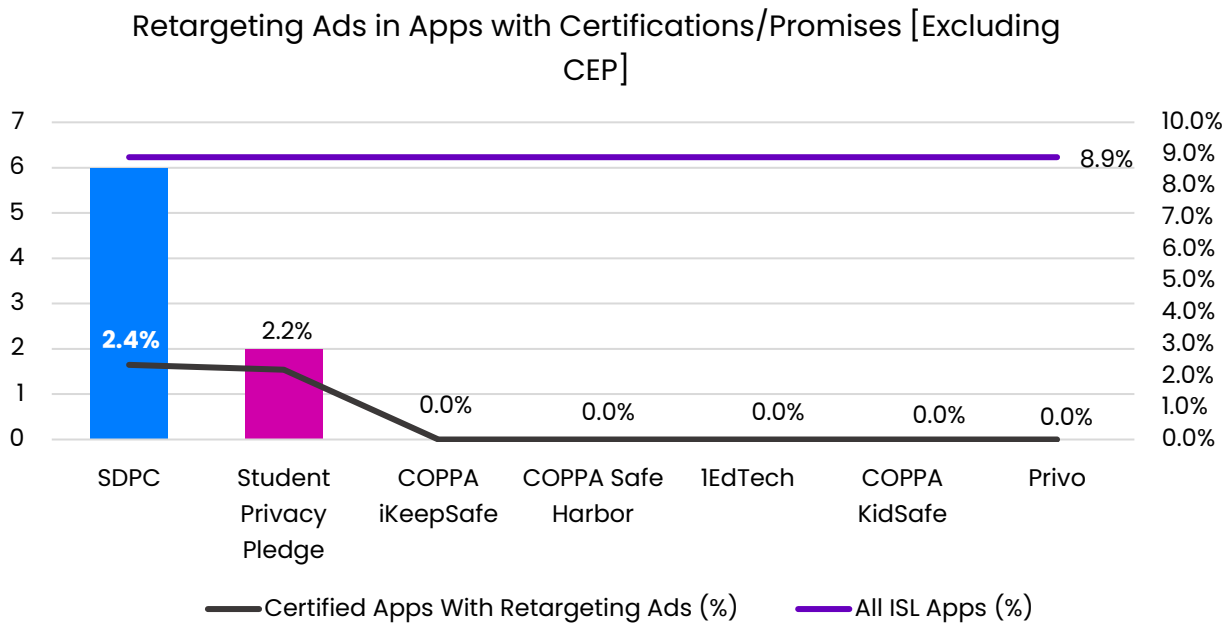


Figure 7.5b

7.2 COPPA Safe Harbor Programs

What is COPPA Safe Harbor?

COPPA Safe Harbor is a program established by the FTC as part of COPPA to enable the industry to regulate itself. The Safe Harbor requirements within the law can be found here.

What does Safe Harbor Certification entail?

To become an approved safe harbor program, participants must implement requirements that are better or substantially similar to COPPA's requirements, provide for effective and mandatory mechanisms for independent assessments, and effectively incentivize compliance.[xviii]

Safe Harbor Programs can meet the independent assessment requirement by conducting periodic reviews on a regular or random basis. But at minimum, a comprehensive review by the safe harbor program of the vendor's information policies, practices and representations must be conducted annually.

[xviii] COPPA, 16 C.F.R. 312.10(b) https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

Apps must be reviewed at least annually to ensure that the technology is upholding all the protections contained in COPPA.

Who Can Perform COPPA Safe Harbor Testing?

Currently, the FTC has approved six COPPA Safe Harbor Programs. These programs are: iKeepSafe, KidSafe, PRIVO, TRUSTe, ESRB, and CARU.

7.2.1 COPPA Safe Harbor Findings

Our benchmark sample set included apps certified by three of the six COPPA Safe Harbor Programs: iKeepSafe, KidSafe and Privo. No apps certified by TRUSTe, ESRB, or CARU were included in the sampled apps. In total, 77 apps in our data set were certified by COPPA Safe Harbor programs. This number drops down to 61 when we remove CEP apps.

7.2.1.1 App Scores

Figures 7.6a and 7.6b display the score breakdown for all the apps that have been COPPA Safe Harbor certified in our data set. Surprisingly, these apps scored worse than the overall data set, with 73.8% of the non-CEP apps receiving a "Do Not Use" score, compared to 54.6% in the full sample. There were proportionally fewer High Risk apps in the COPPA Safe Harbor certified apps, which might have been a positive, but in this case, it reflects the case that more apps were scored Do Not Use, and fewer scored Some Risk (there were 0% Some Risk apps in the certified apps vs. 3.9% in the full sample).

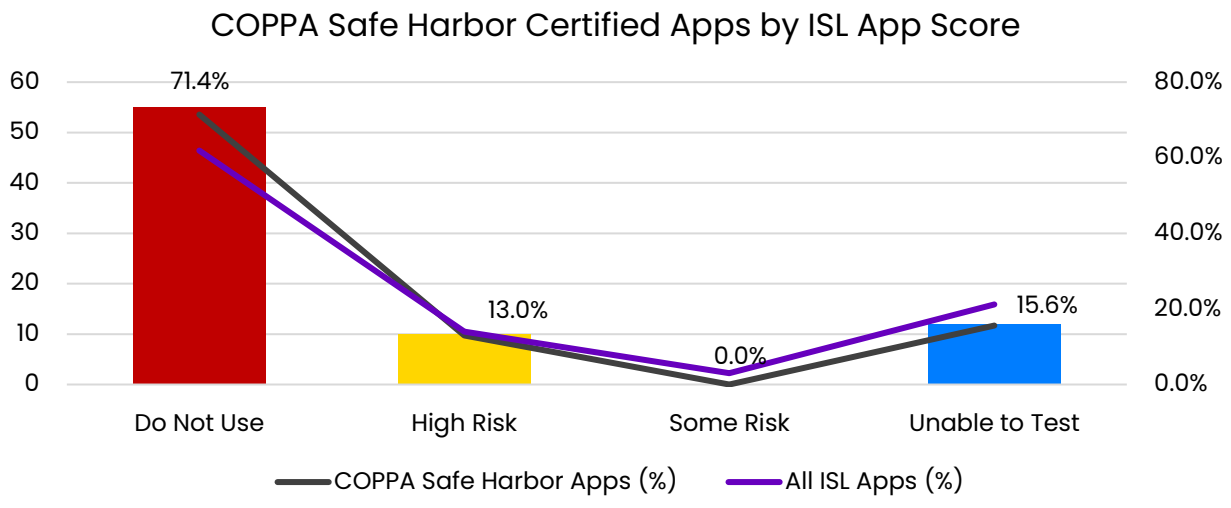


Figure 7.6a

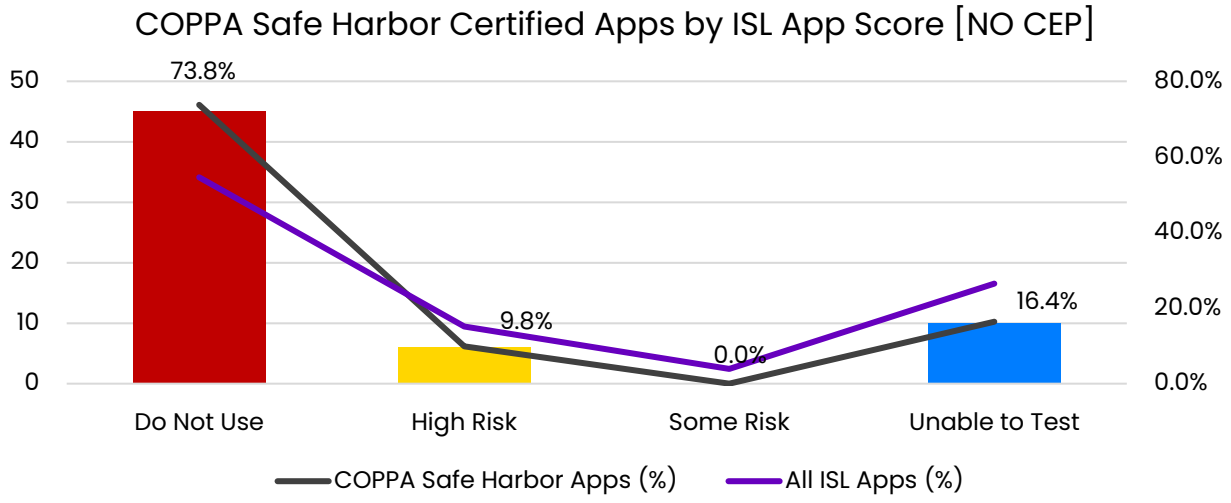


Figure 7.6b

7.2.1.2 Examination of Do Not Use Scores

The significantly higher percent of apps scored Do Not Use (DNU) in the COPPA Safe Harbor apps (73.8%) than both the overall sample (54.6%), and apps without certifications (56.1%) prompted us to look more closely at the DNU score triggers in the COPPA Safe Harbor certified apps (Figures 7.7b and 7.8b). It's a positive finding that the COPPA Safe Harbor DNU apps more frequently had only one DNU criterion than the overall sample set (55.6% compared to 48%). However, the COPPA Safe Harbor DNU apps somewhat more frequently had three Do Not Use criteria than the overall set (17.8% compared to 12.9%).

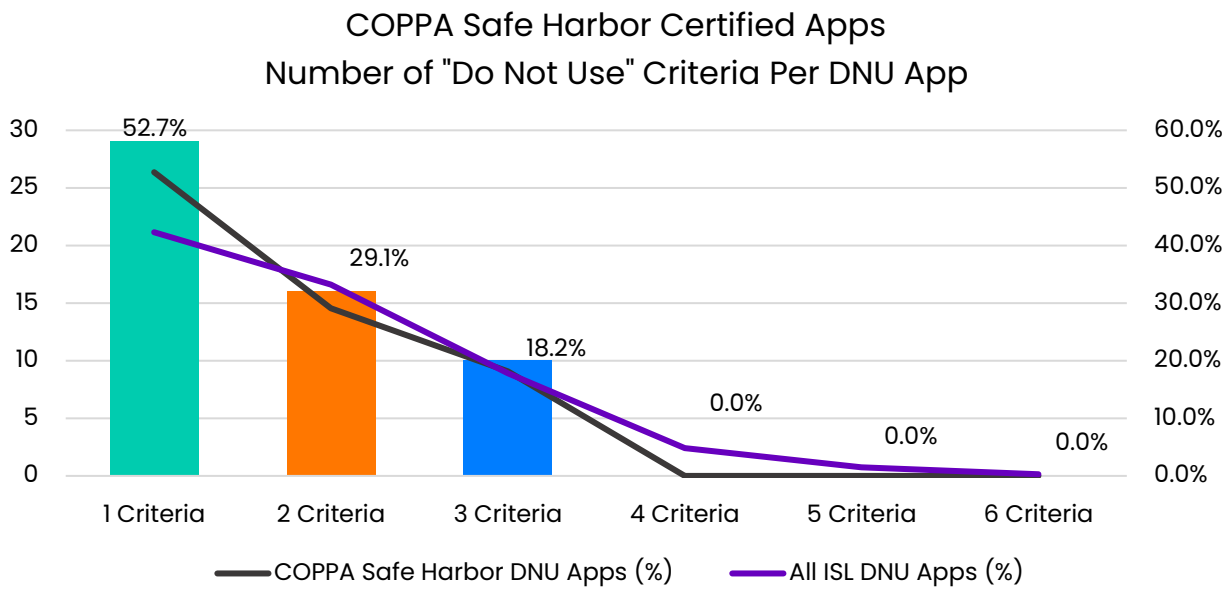


Figure 7.7a

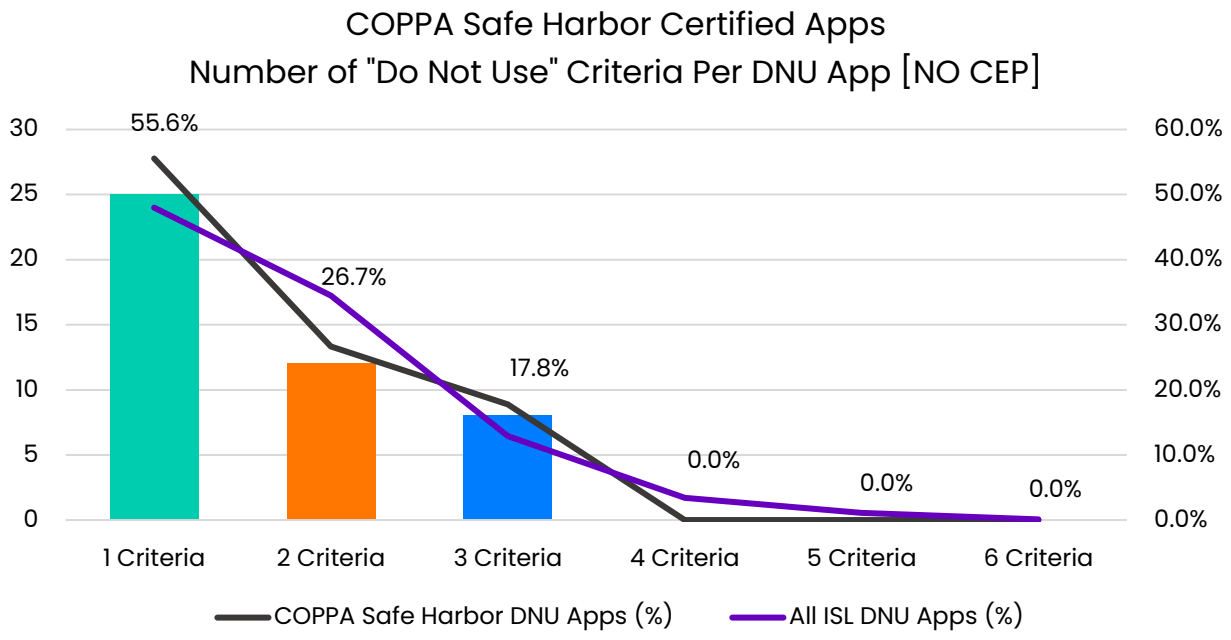


Figure 7.7b

In terms of specific DNU criteria (Figure 7.8b), COPPA Safe Harbor certified apps scored DNU only had a single criterion that was higher in likelihood—and then only marginally so—than the overall sample set: advertising (21.6% vs. 20.5%), but

it is disappointing to see this. Other interesting findings in the set of COPPA Safe Harbor certified apps with DNU scores:

- 37.3% of the COPPA Safe Harbor apps with DNU scores were observed sending information to Facebook.
    - 51.0% of these apps include Facebook SDKs.
- Nearly 40% of COPPA Safe Harbor apps had traffic going to Twitter, compared to only 18.7% of the total sample set.

31.5% of COPPA Safe Harbor apps included advertising, compared to 22.4% of the total sample set.

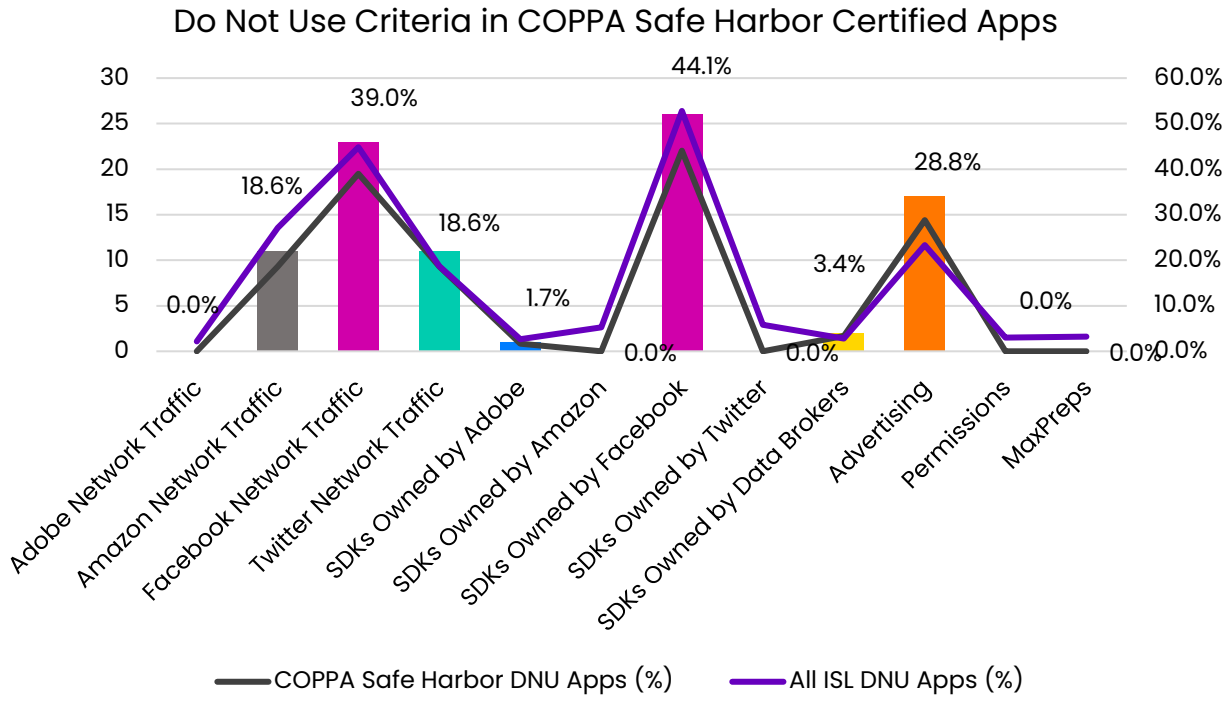


Figure 7.8a

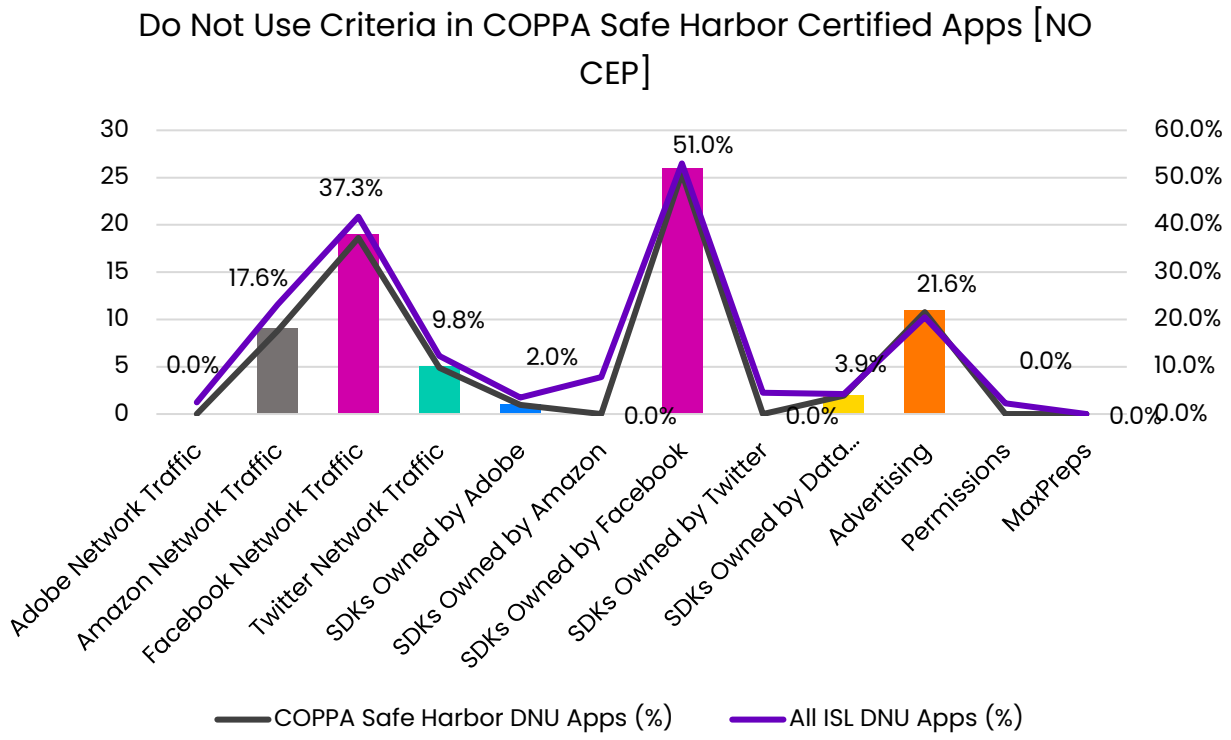


Figure 7.8b

7.2.1.3 Advertising Presence

As can be seen from Figure 7.9b below, COPPA Safe Harbor certified apps were more likely to contain digital ads and retargeting ads than the total sample set (21.6% of COPPA Safe Harbor apps vs. 15.2% of the overall data set). This is unexpected and an indication that, while COPPA Safe Harbor certification may uphold the letter of the law, it is not keeping students as safe as it could. ISL hopes that future regulation better addresses the substantial data sharing risks inherent in the current digital advertising architectures.

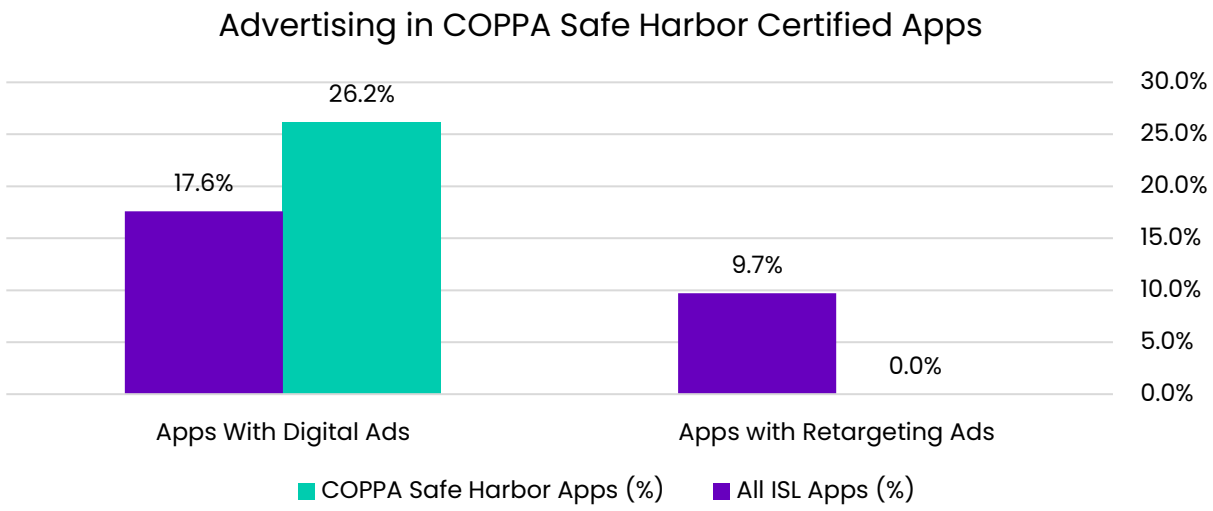


Figure 7.9a

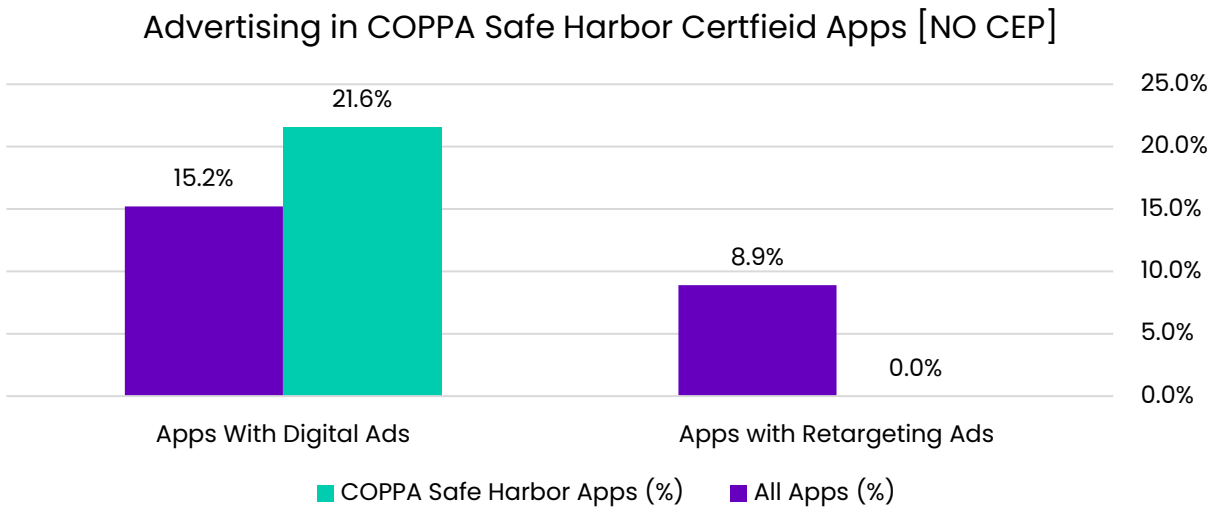


Figure 7.9b

7.2.1.4 Most Recommended COPPA Safe Harbor Apps

Figure 7.10 shows the most recommended COPPA Safe Harbor certified apps in the sample based on frequency of use across all schools in the sample.

The colors in the chart reflect the app safety score. (Red = DNU, Yellow = High Risk, Green = Some Risk, Blue = Unable to Test/Untested/Unscored.)

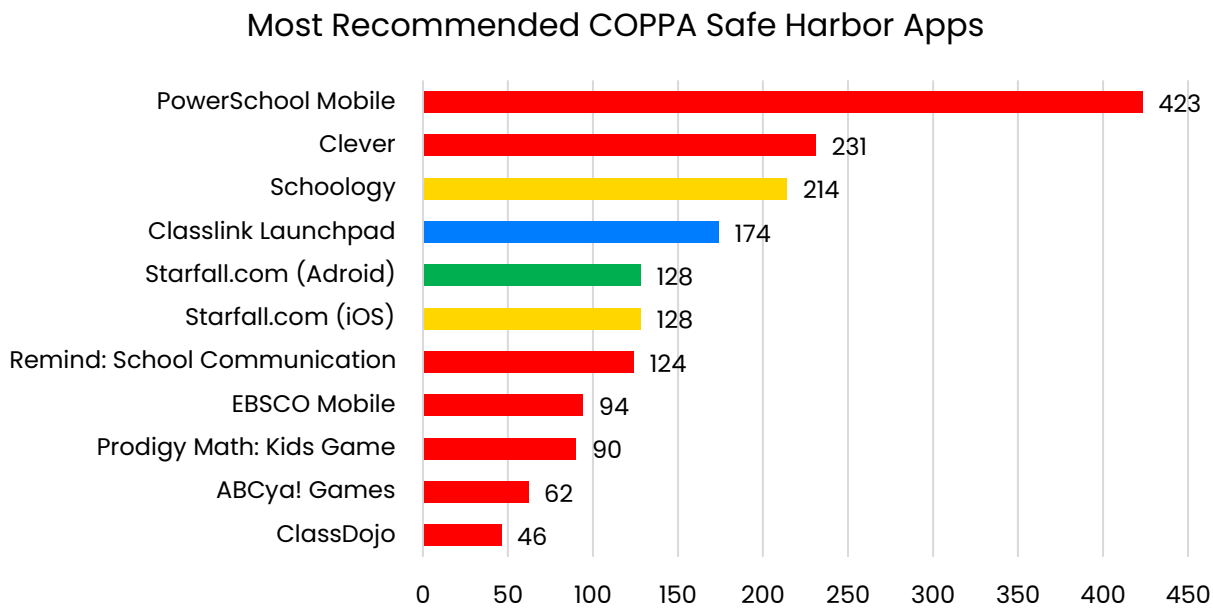


Figure 7.10

7.2.2 iKeepSafe COPPA Certification

There were 40 iKeepSafe COPPA certified apps in our sample, dropping to only 24 apps when removing CEP apps.

7.2.2.1 App Scores

Of the three Safe Harbor programs, this program had the highest percentage of Do Not Use apps with 79.2% of the certified apps (Figure 7.11b). This is substantially higher than the percentage of DNU apps in the overall sample set (54.6%).

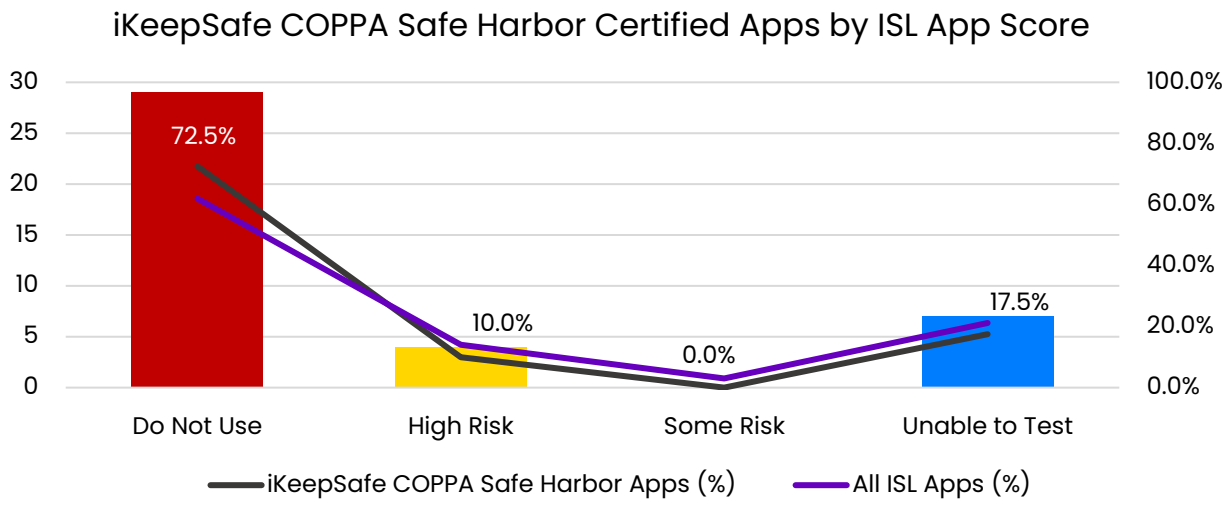


Figure 7.11a

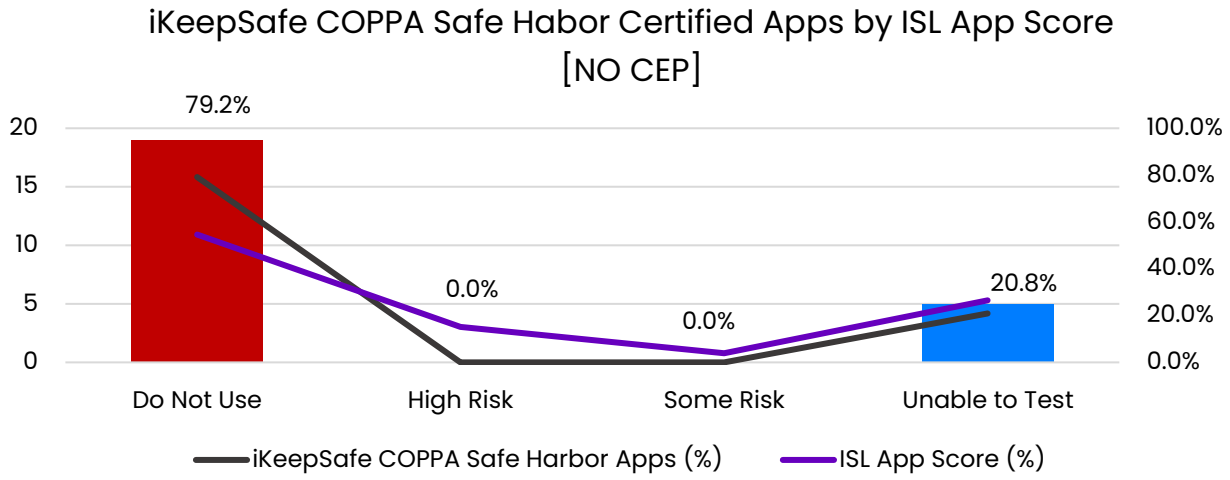


Figure 7.11b

7.2.2.2 Examination of Do Not Use Scores

The iKeepSafe DNU apps performed better than the overall sample set with respect to the number of DNU criteria. The iKeepSafe DNU apps had a significantly

higher percentage of apps with only one DNU criteria (48.0% vs. 84.2%) and substantially fewer apps with two or more DNU criteria.

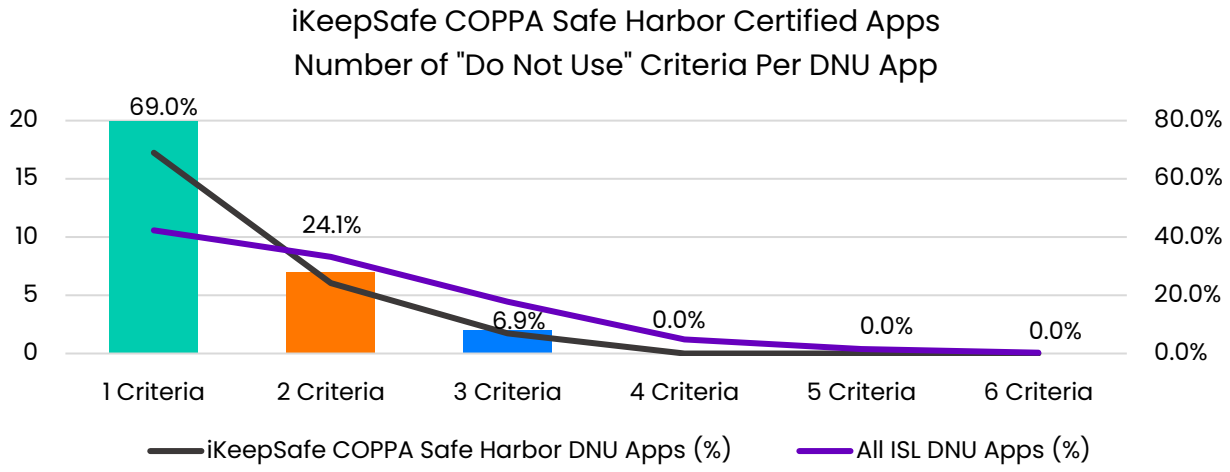


Figure 7.12a

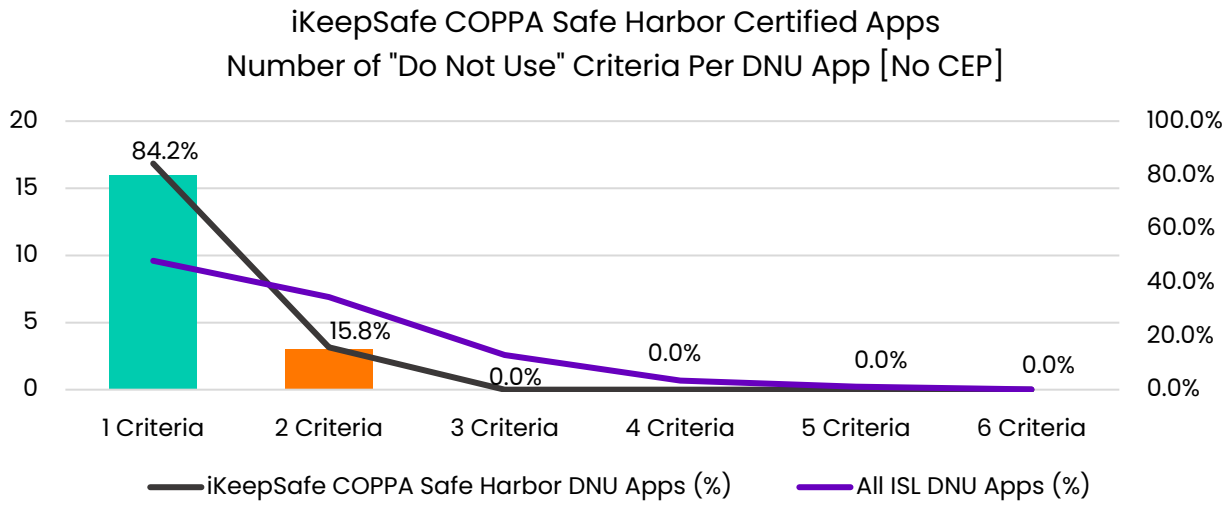


Figure 7.12b

Figure 7.13b shows the breakdown of DNU triggers found in the iKeepSafe DNU apps. All the triggers were less likely in the iKeepSafe DNU apps except for the presence of Facebook SDKs (57.9% vs. 53.0% in the overall set of DNU apps).

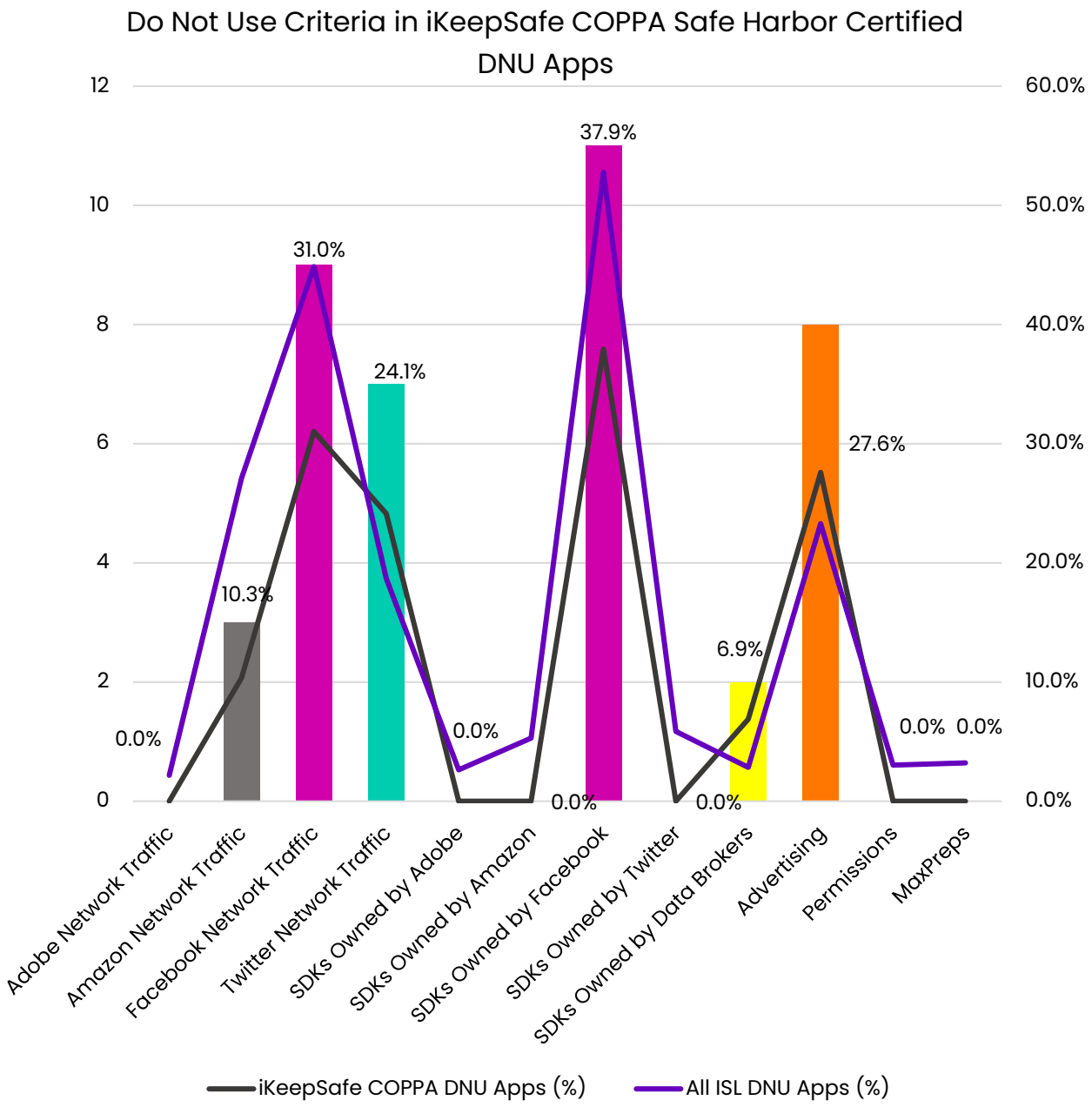


Figure 7.13a

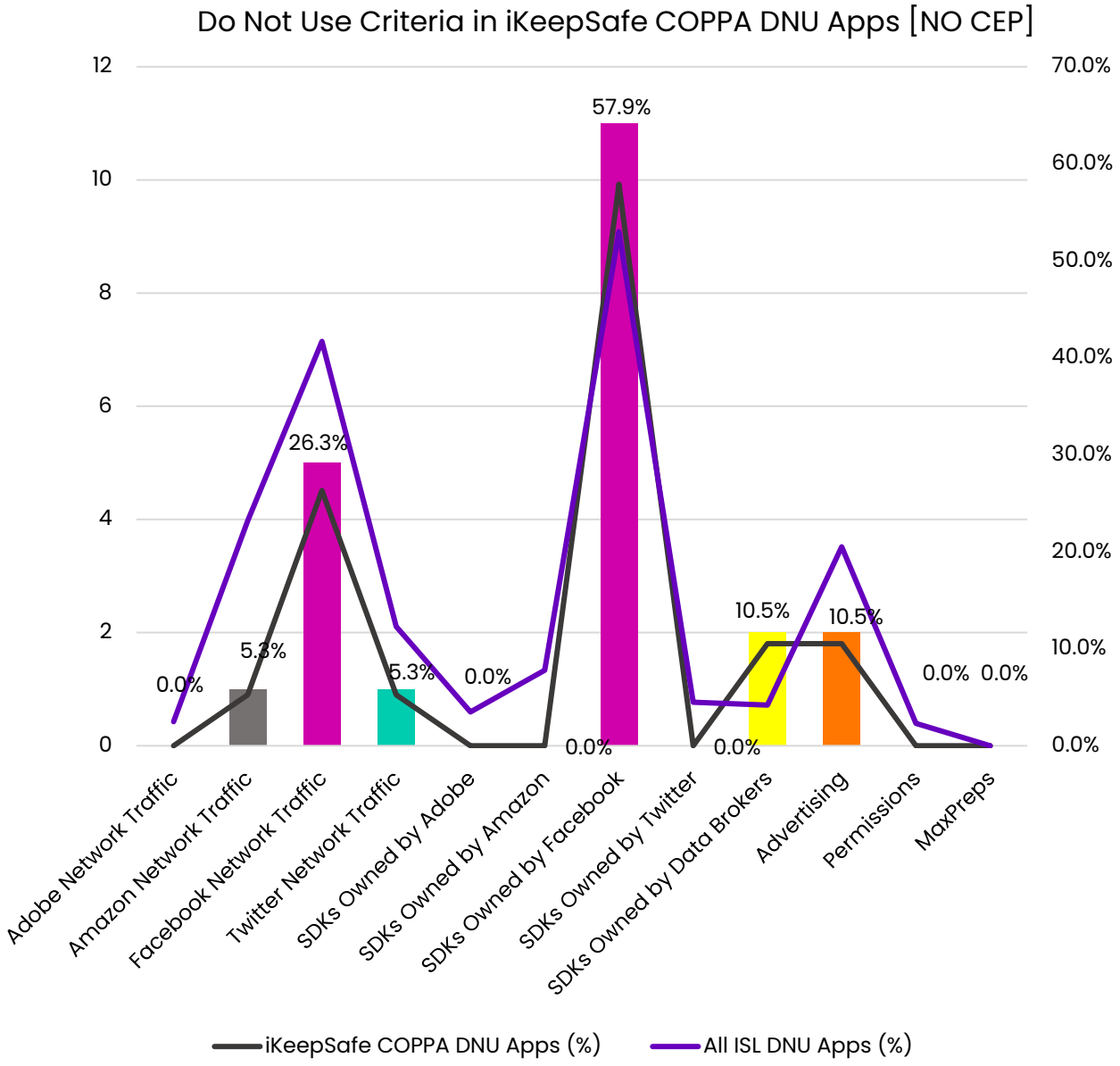


Figure 7.13b

7.2.2.3 Advertising Presence

iKeepSafe COPPA Safe Harbor certified apps were less likely to have ads than the overall sample set (10.5% vs 15.2%), and the certified apps had no retargeting ads. (Figure 7.14b).

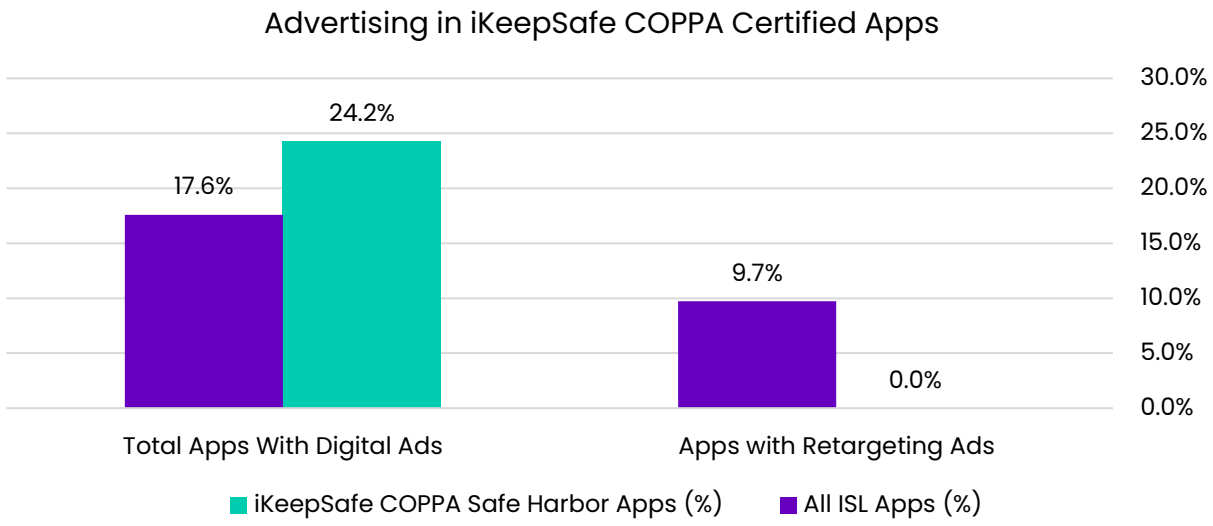


Figure 7.14a

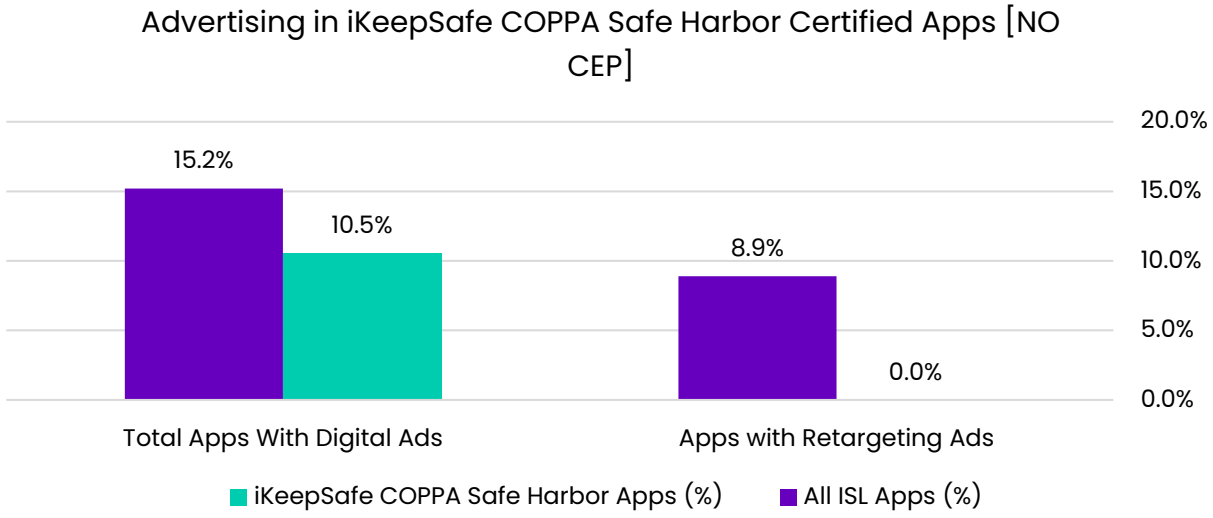


Figure 7.14b

7.2.2.4 Most Recommended iKeepSafe COPPA Safe Harbor Certified Apps

Figure 7.15 shows the most recommended iKeepSafe COPPA Safe Harbor certified apps in the sample based on frequency of use across all schools in the sample.

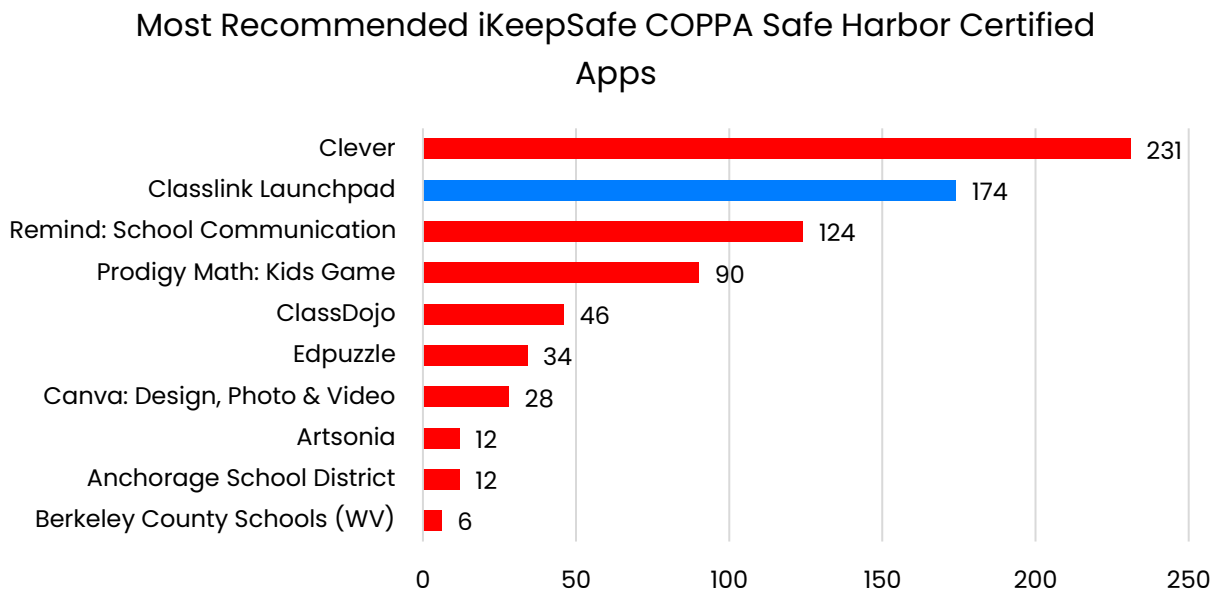


Figure 7.15

7.2.3 KidSafe COPPA Certification

There were only 25 KidSafe COPPA Certified apps in the sample and **none** of these were CEP apps. We were able to test proportionally more of these than the overall sample set, with only 12.0% unable to test, compared to 26.5% in the overall sample.

7.2.3.1 App Scores

The number of KidSafe apps is inadequate to draw any conclusions, but we note the performance compared to the total sample set. Overall, the KidSafe COPPA certified apps performed worse in safety scores than the overall data set with a higher percentage of Do Not Use apps (72.0% vs 54.6%, Figure 7.16).

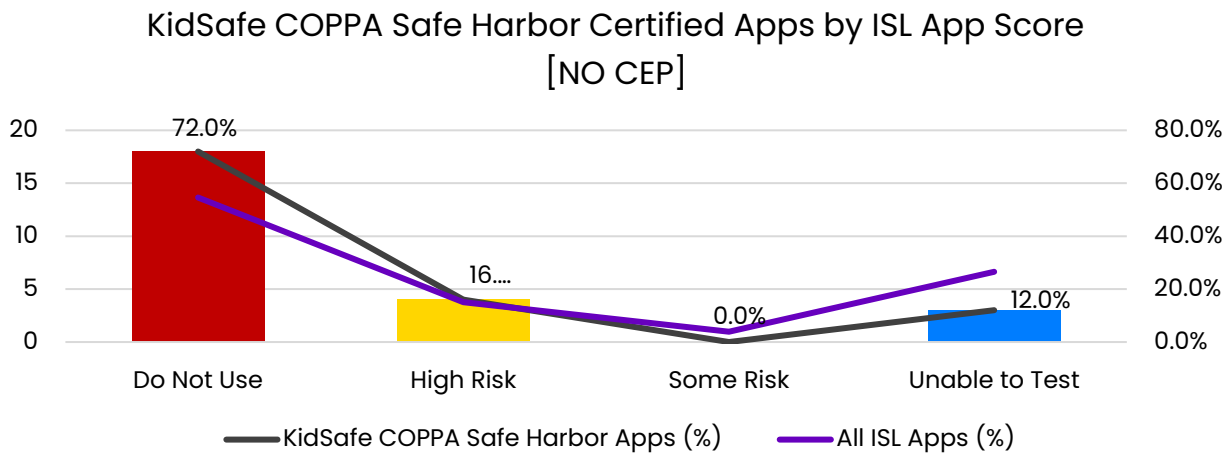


Figure 7.16

7.2.3.2 Examination of Do Not Use Scores

Unlike the iKeepSafe apps, the KidSafe apps had a *higher* percentage of DNU apps with two and three DNU criteria (Figure 7.17). This undesirable finding warrants evaluating a larger number of KidSafe apps.

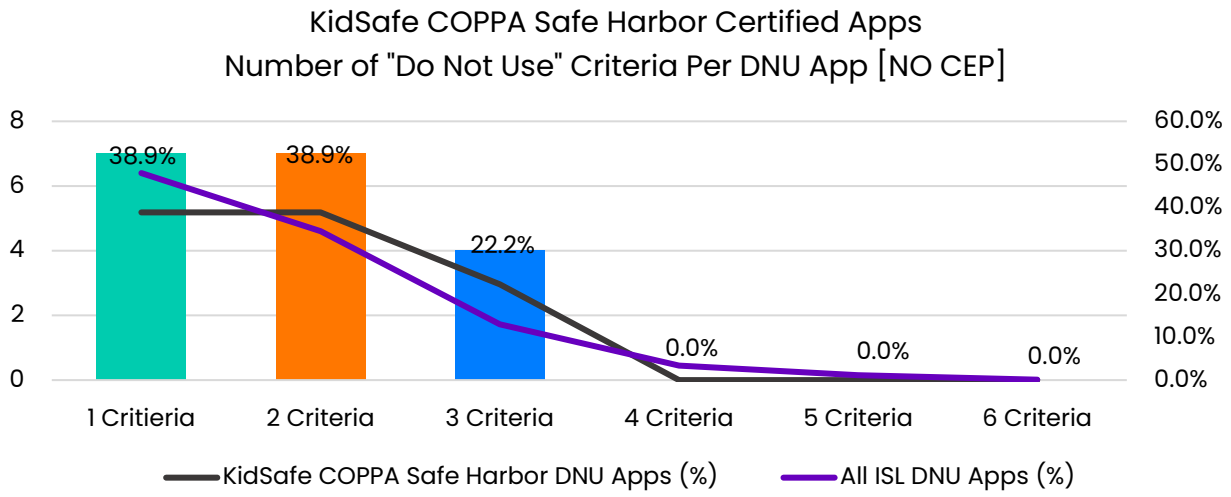


Figure 7.17

In similar fashion, we observe more Amazon, Facebook, and Twitter network traffic in the KidSafe COPPA Safe Harbor certified apps (Figure 7.18), underscoring the need for additional analysis.

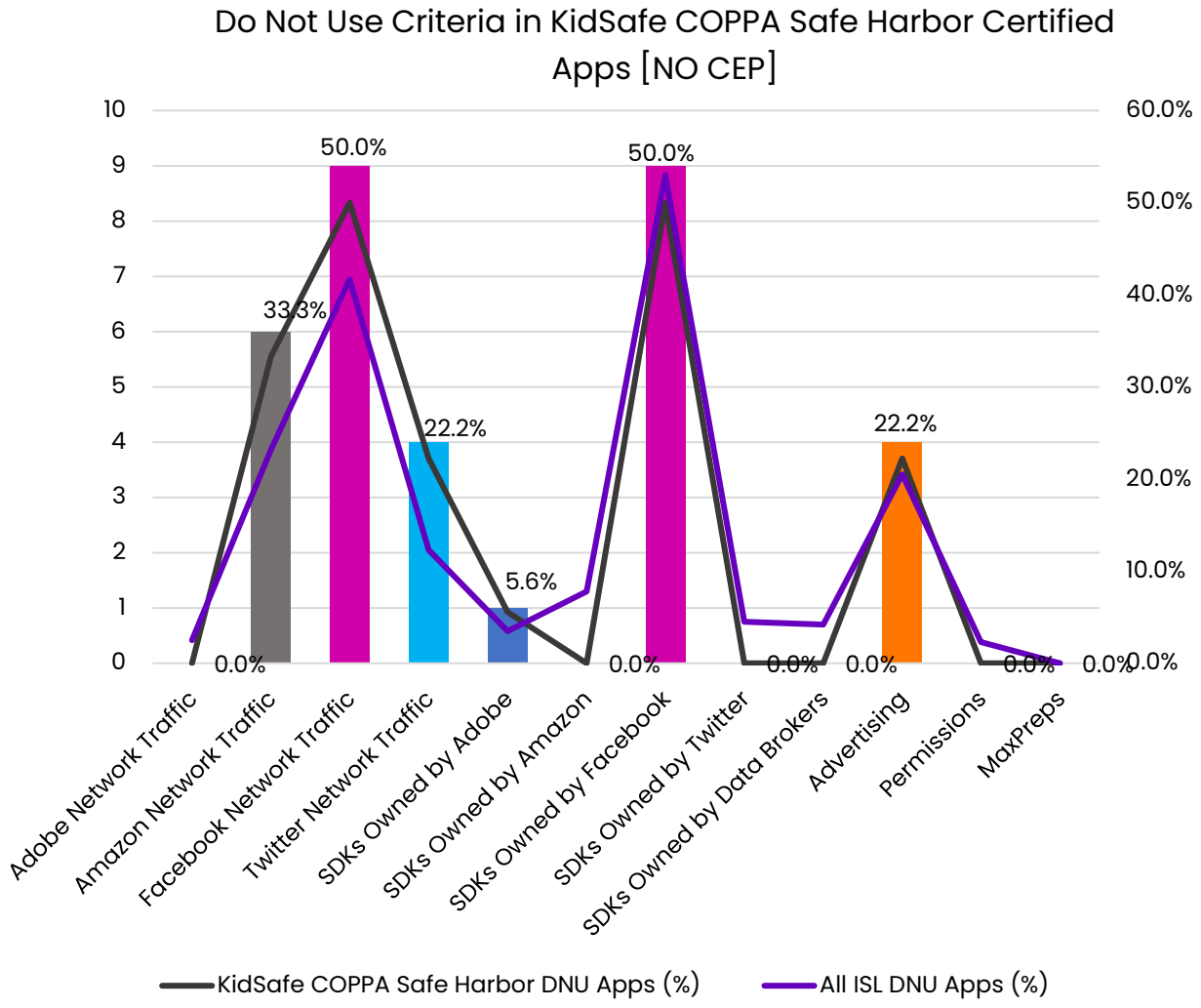


Figure 7.18

7.2.3.3 Advertising Presence

KidSafe COPPA Safe Harbor certified apps contain more digital ads than the overall sample set (18.2% compared to 15.2%, Figures 7.19a and 7.19b) but contained no retargeting ads. Note that two charts are shown: Figure 7.19a compares the KidSafe COPPA Safe Harbor certified apps against *all* apps and Figure 7.19b compares the KidSafe COPPA Safe Harbor certified apps against all *non-CEP* apps.

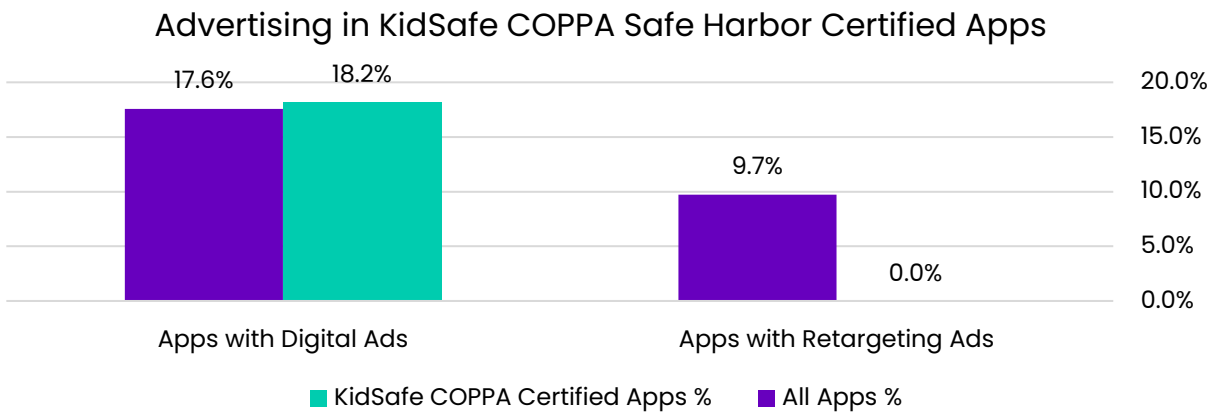


Figure 7.19a

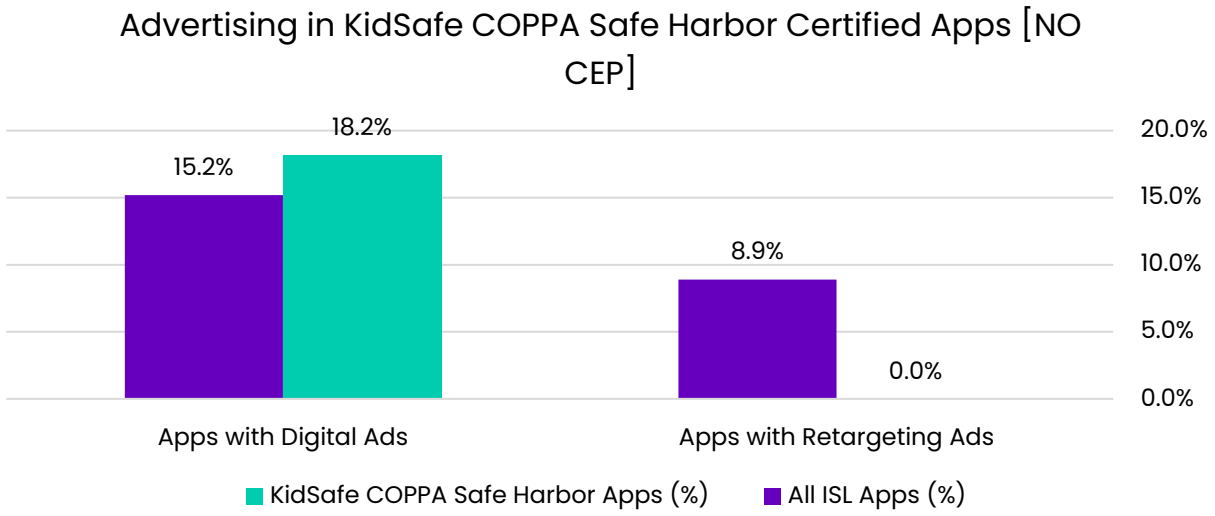


Figure 7.19b

7.2.3.4 Most Recommended KidSafe COPPA Safe Harbor Certified Apps

Figure 7.20 shows the most recommended KidSafe COPPA Safe Harbor certified apps in the sample based on frequency of use across all schools in the sample.

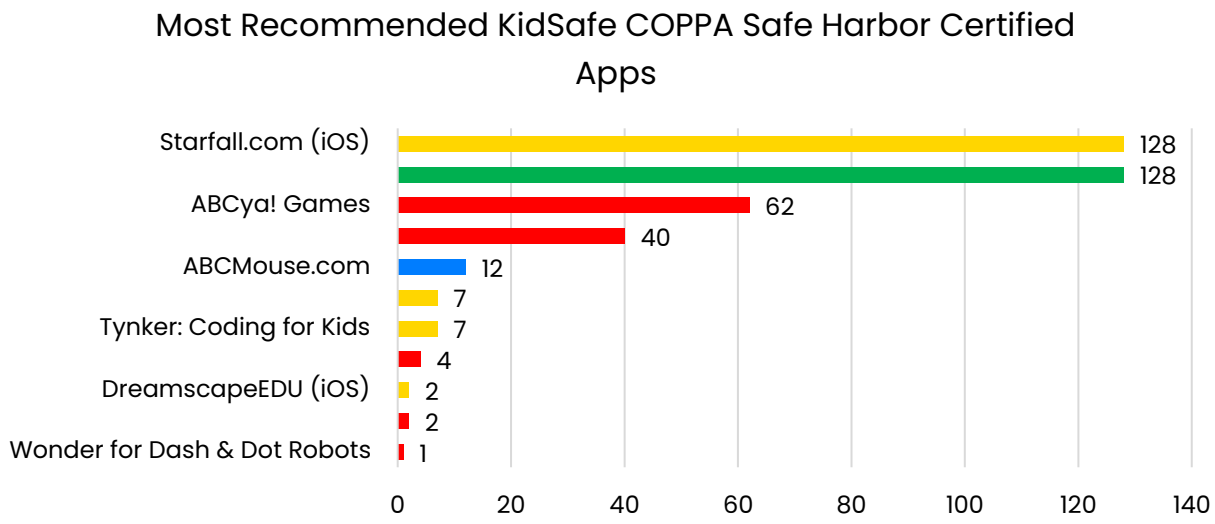


Figure 7.20

7.2.4 PRIVO COPPA Certification

There were only ten PRIVO COPPA certified apps in the sample and **no** CEP apps. Like the KidSafe sample, this is too small to be statistically meaningful, but we include these detailed findings for completeness.

7.2.4.1 App Scores

The studied sample of PRIVO COPPA Safe Harbor certified apps had a significantly higher percentage of DNU and High Risk apps than the overall sample set.

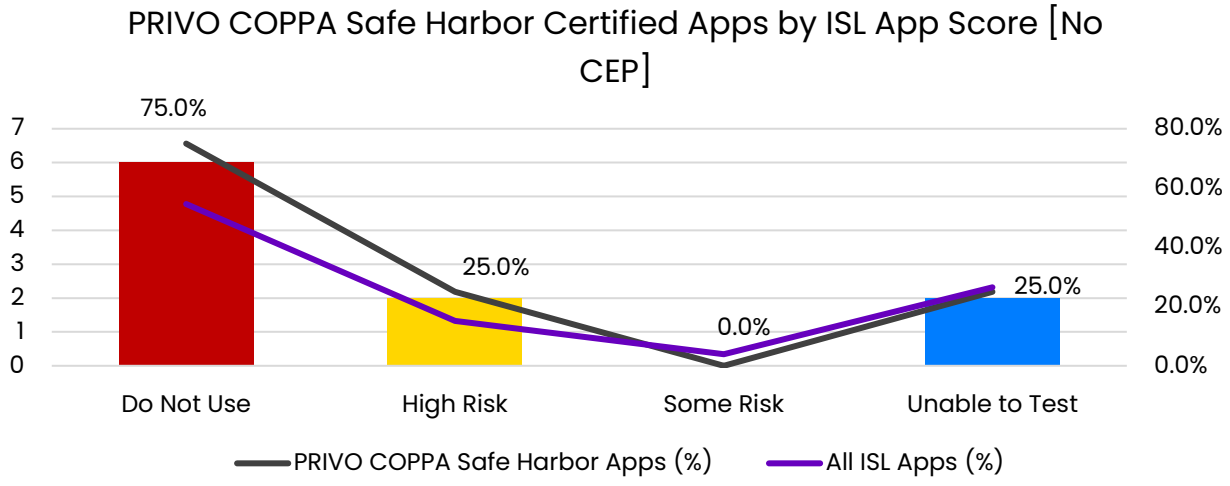


Figure 7.21

7.2.4.2 Examination of Do Not Use Scores

Half of the PRIVO COPPA certified apps with DNU scores had 3 DNU triggers (Figure 7.22).

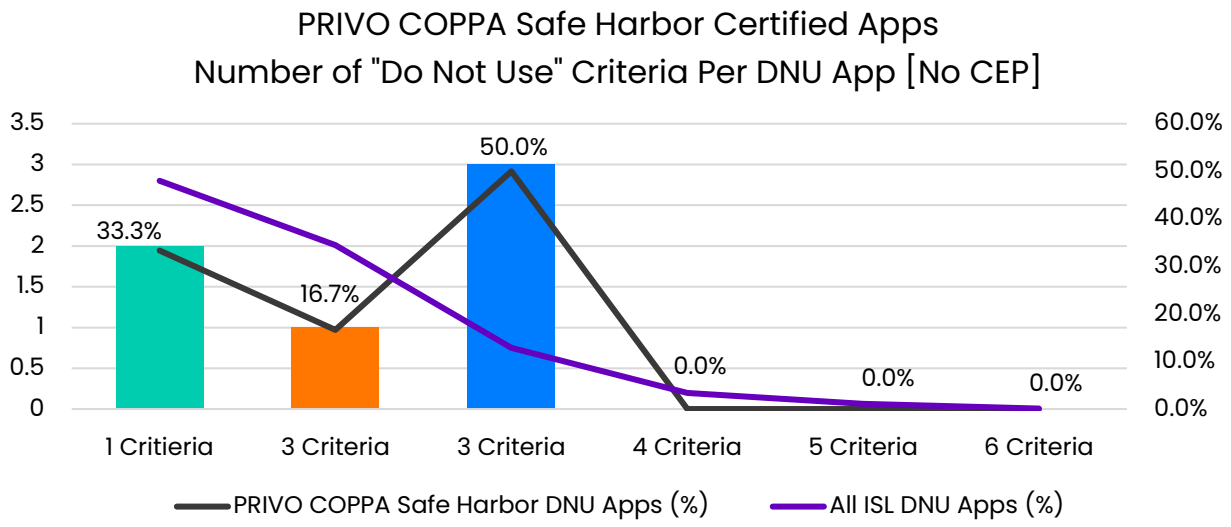


Figure 7.22

Two-thirds of the PRIVO COPPA certified apps with DNU scores received that score due to the presence of Facebook SDKs and ads (Figure 7.23).

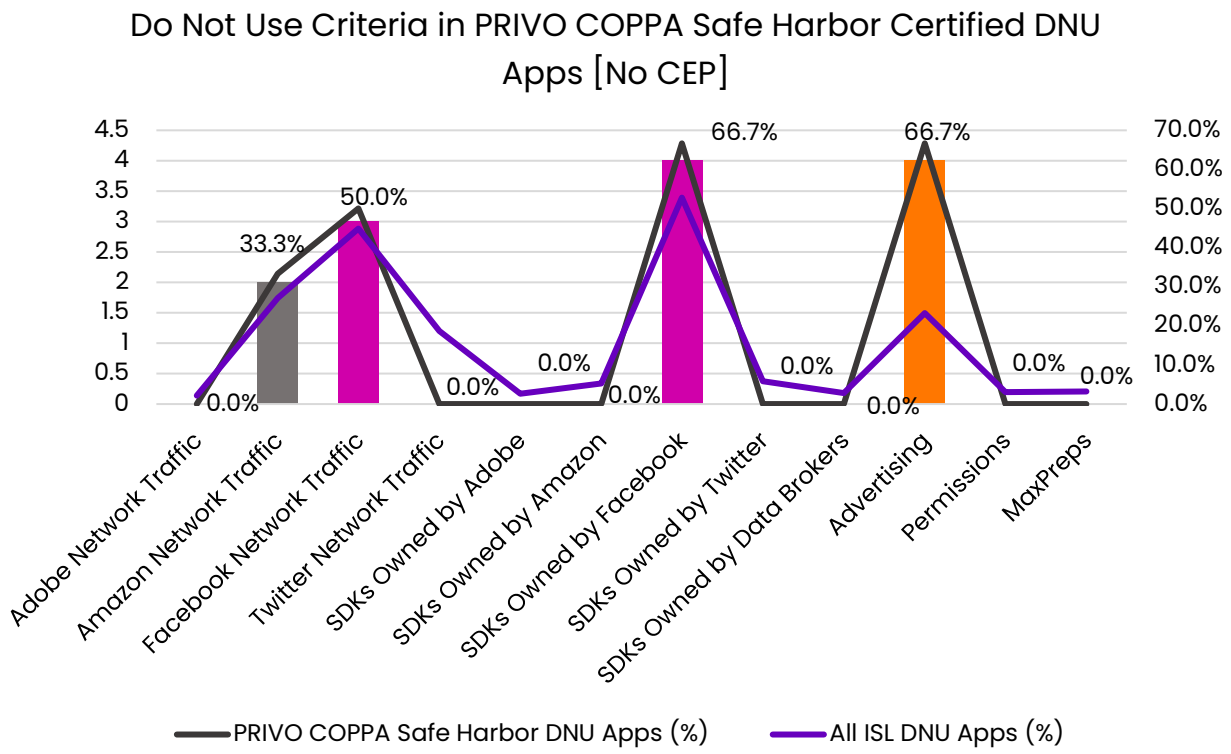


Figure 7.23

7.2.4.3 Advertising Presence

Fifty percent of the PRIVO COPPA Safe Harbor certified apps had digital ads—substantially higher than the overall data set. None of the PRIVO COPPA certified apps had retargeting ads (Figure 7.24).

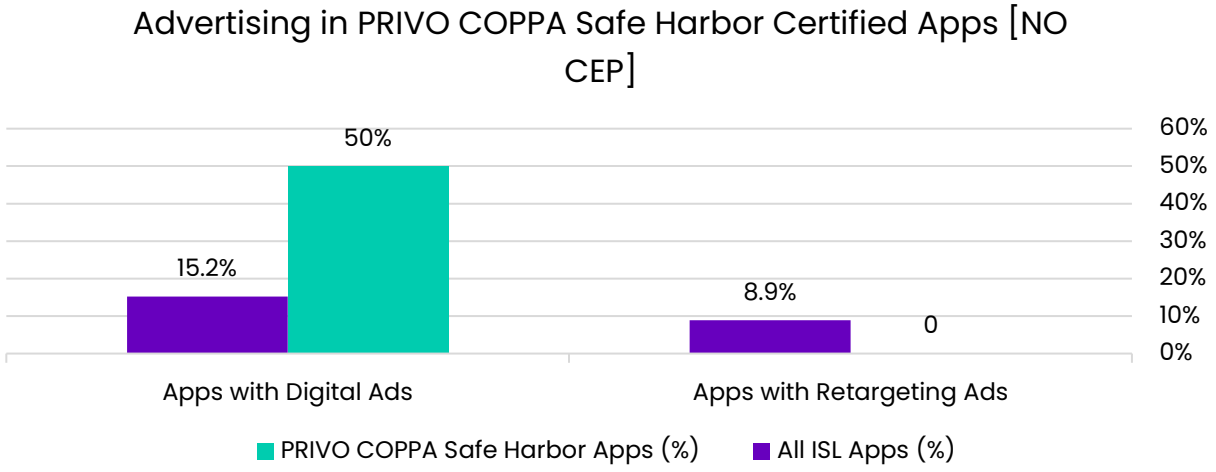


Figure 7.24

7.2.4.4 Most Recommended PRIVO COPPA Safe Harbor Certified Apps

Figure 7.25 shows the most recommended PRIVO COPPA Safe Harbor certified apps in the sample based on frequency of use across all schools in the sample.

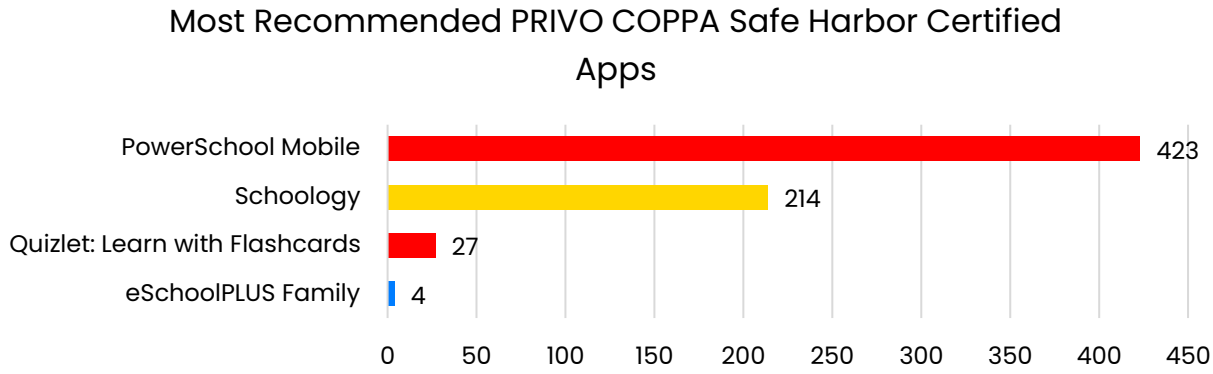


Figure 7.25

7.3 Proprietary Certifications

Other certification seals by corporations or nonprofits that are not approved COPPA Safe Harbor programs fall under this category. There is only one certification program that falls in this category in our dataset: 1EdTech certification.

7.3.1 1EdTech Certification

There were 42 1EdTech certified apps in the dataset; removing CEP apps leaves 40 apps in this subset of apps. Nearly fifty percent (47.5%) of apps were unable to be tested, compared to 26.5% in the overall data set.

7.3.1.1 App Scores

Overall, 1EdTech certified apps performed better than the overall sample set for Do Not Use apps (40.0% compared to 54.6%), and worse on Some Risk apps (0.0% vs 3.9%).

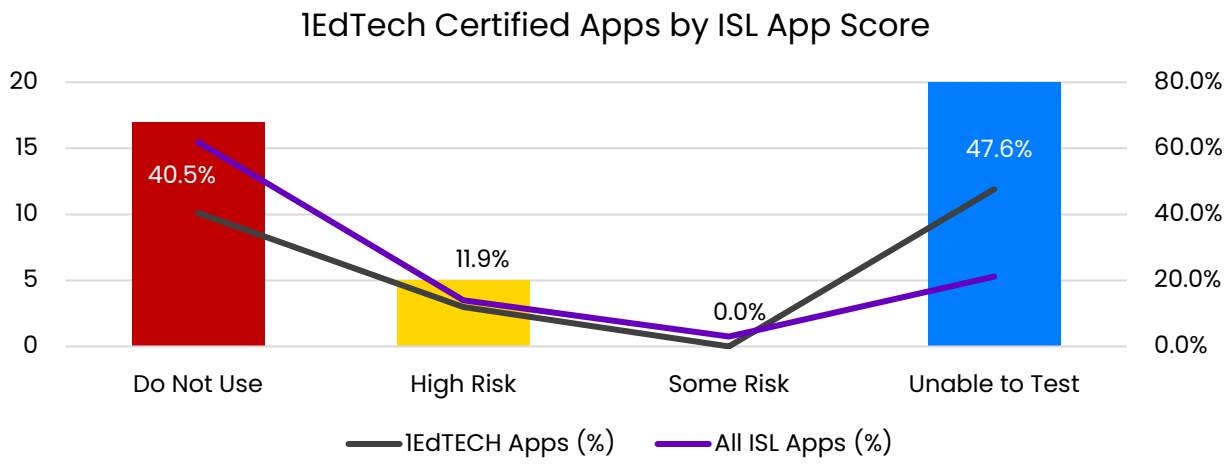


Figure 7.26a

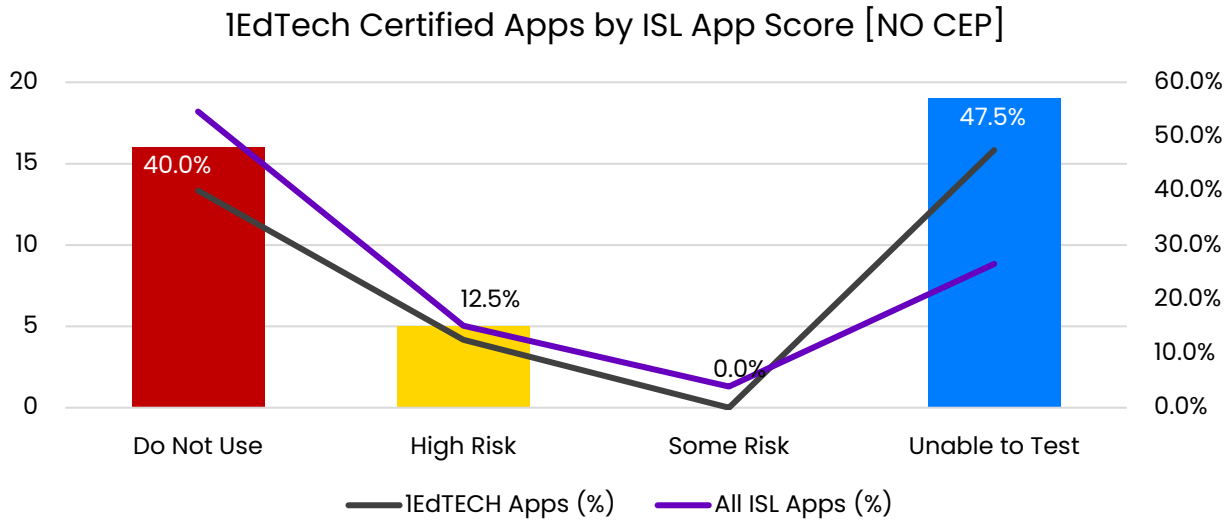


Figure 7.26b

7.3.1.2 Examination of Do Not Use Scores

The 1EdTech certified sample had a much higher percent of DNU apps with only a single DNU criteria and substantially lower percent of multi-criteria for DNU (Figure 7.27b). As noted earlier, this is viewed as a positive.

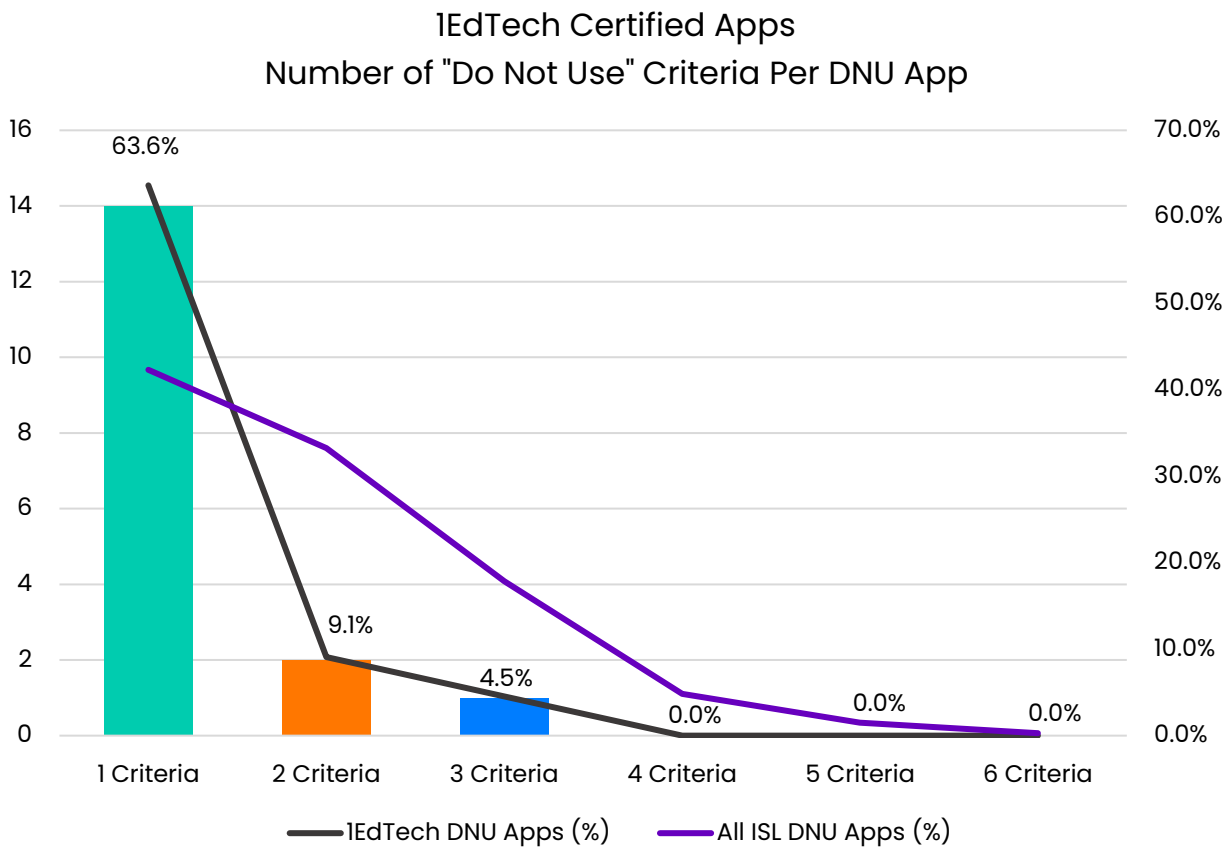


Figure 7.27a

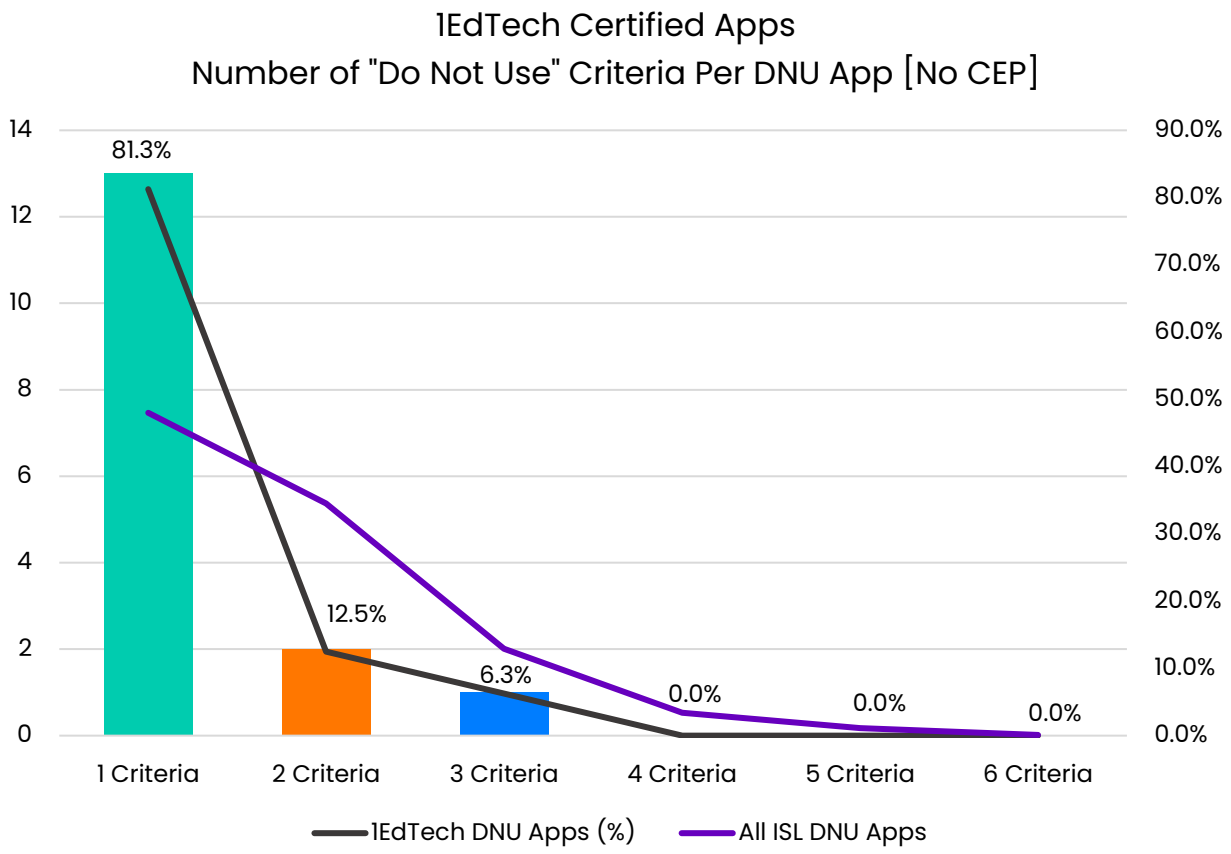


Figure 7.27b

Of note, the 1EdTech certified apps with DNU scores were much more likely to include Facebook network traffic than the overall data set (43.8% vs. 23.2%, Figure 7.28b).

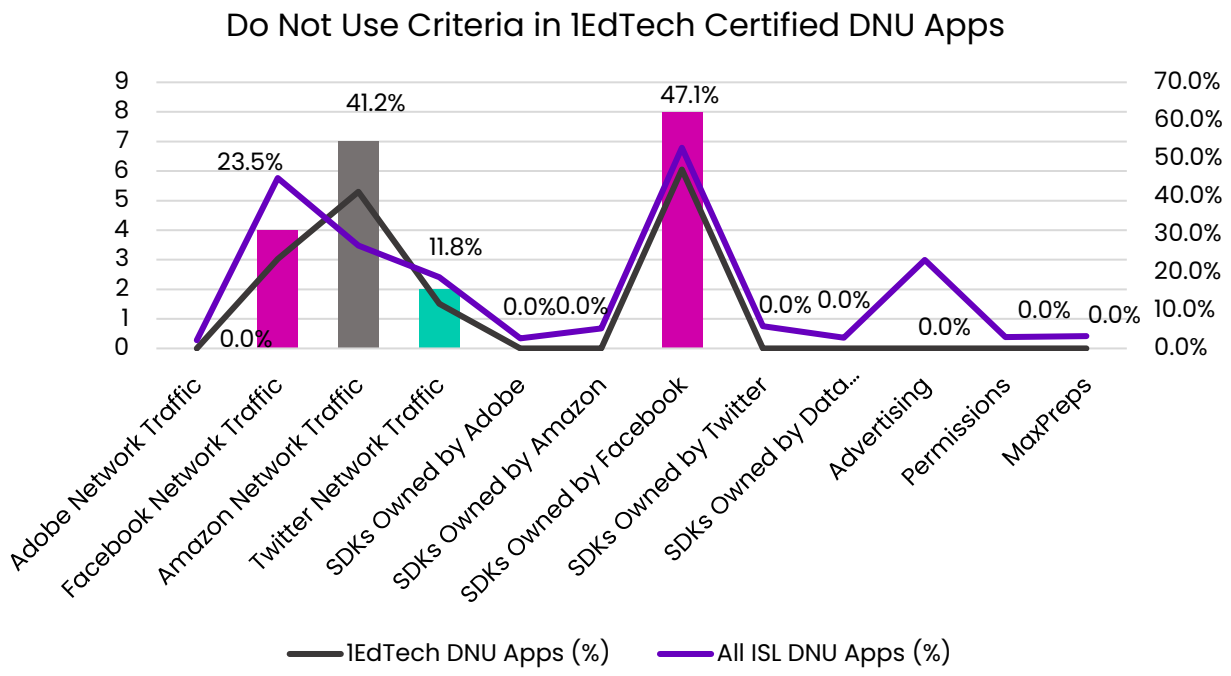


Figure 7.28a

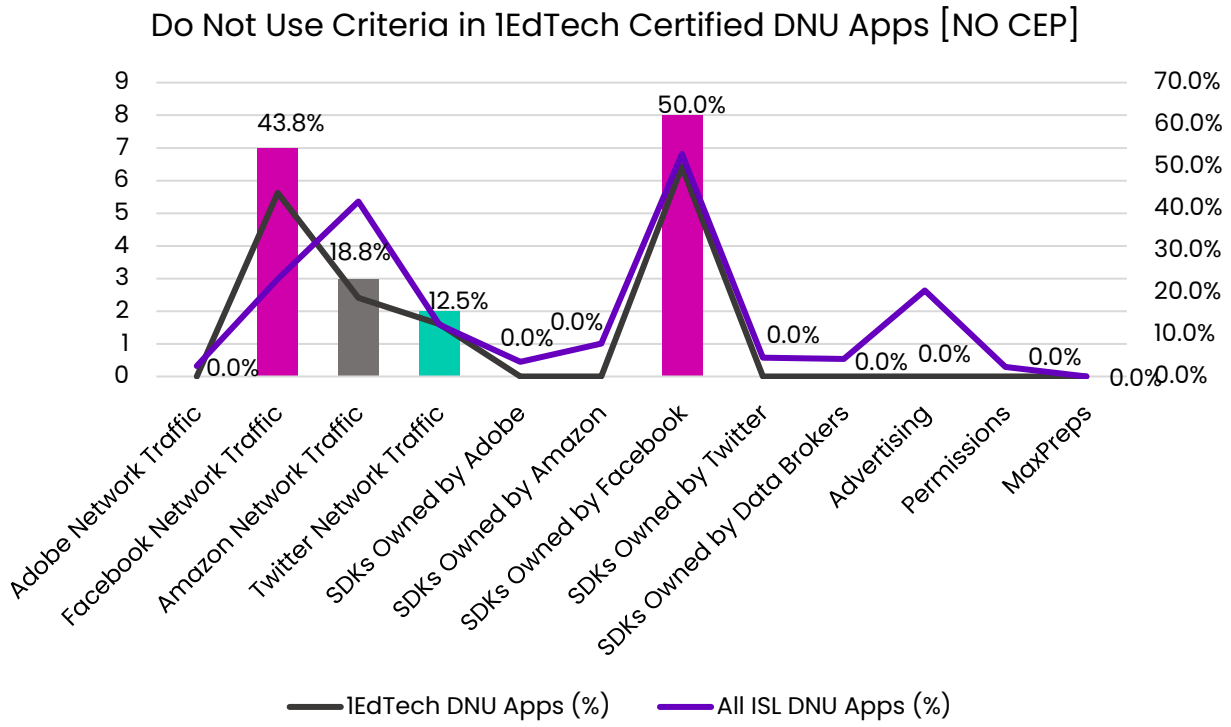


Figure 7.28b

7.3.1.3 Advertising Presence

The 1EdTech certified apps had no ads and no retargeting ads observed, substantially better than the overall dataset (Figures 7.29a and 7.29b).

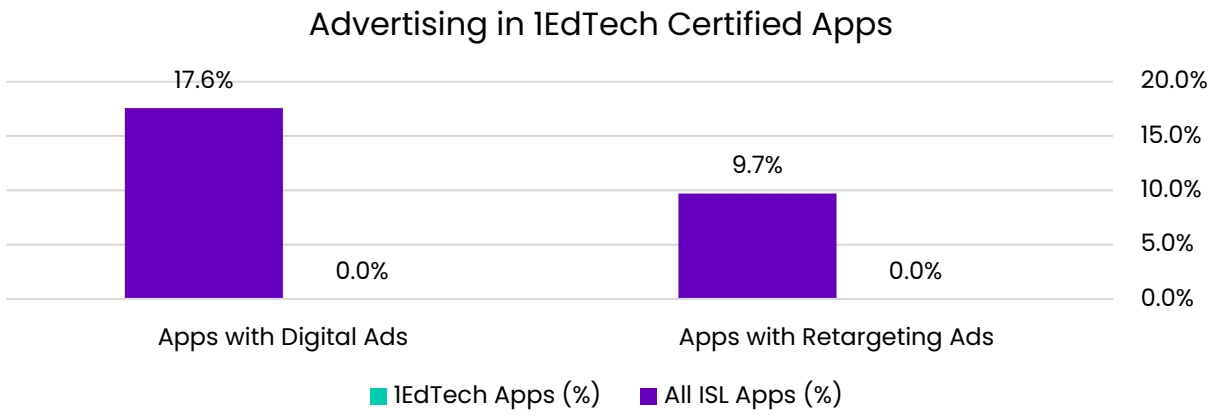


Figure 7.29a

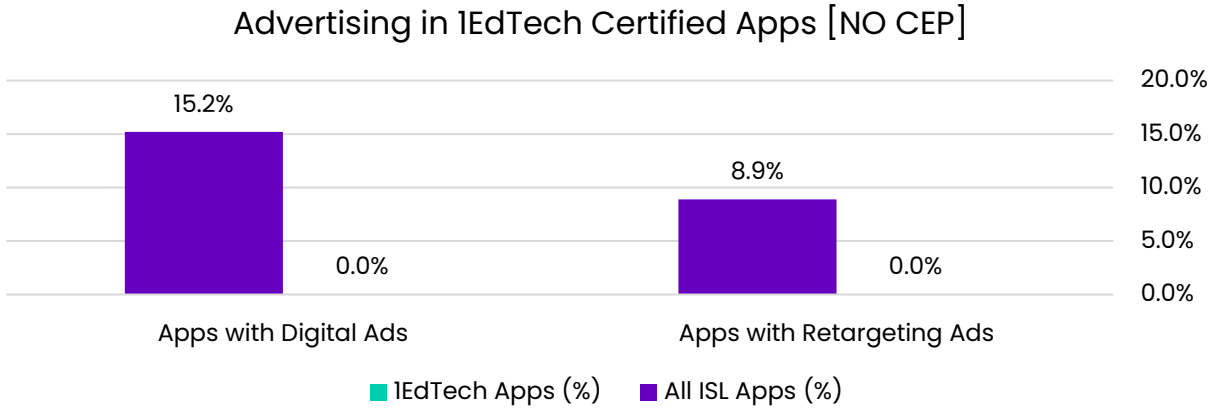


Figure 7.29b

7.3.1.4 Most Recommended 1EdTech Certified Apps

Figure 7.30 shows the most recommended 1EdTech certified apps in the sample based on frequency of use across all schools in the sample.

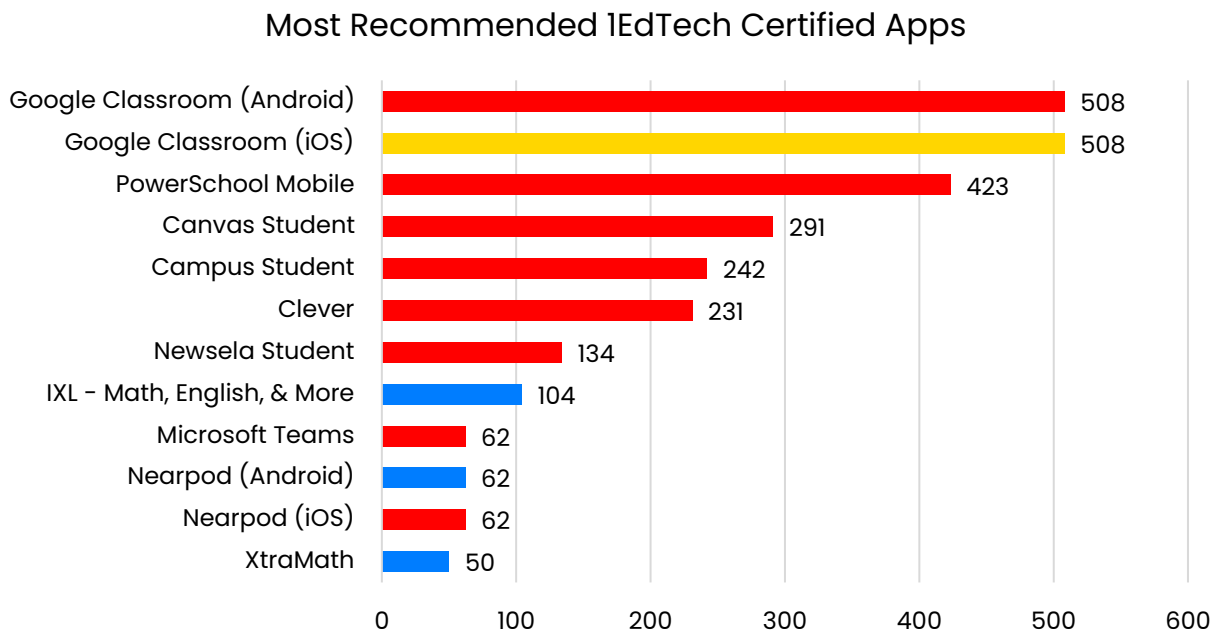


Figure 7.30

7.4 COPPA Compliant Self-Assertions

This section covers apps that were self-asserted as COPPA Compliant by the developer, without evidence of an external certification. These assertions were found in the app's privacy policy.

7.4.1 Findings

Self-asserted COPPA compliant apps were the largest subset of studied apps at 415 apps, dropping to 239 when CEP apps were removed. Overall, this set of apps:

- performed about the same as the overall data set,
- performed better than apps without any certification or promise, and
- performed worse than apps with a certification or promise.

7.4.1.1 App Scores

As can be seen in Figure 7.31b, the self-asserted COPPA compliant apps performed nearly identically to the overall data set with respect to ISL safety score.

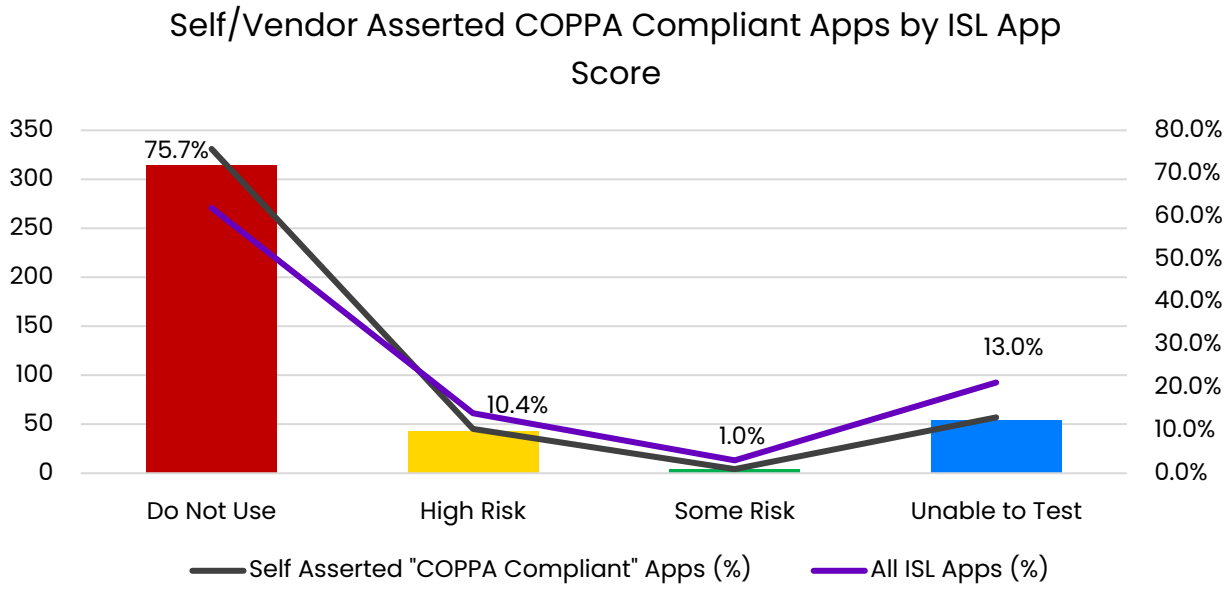


Figure 7.31a

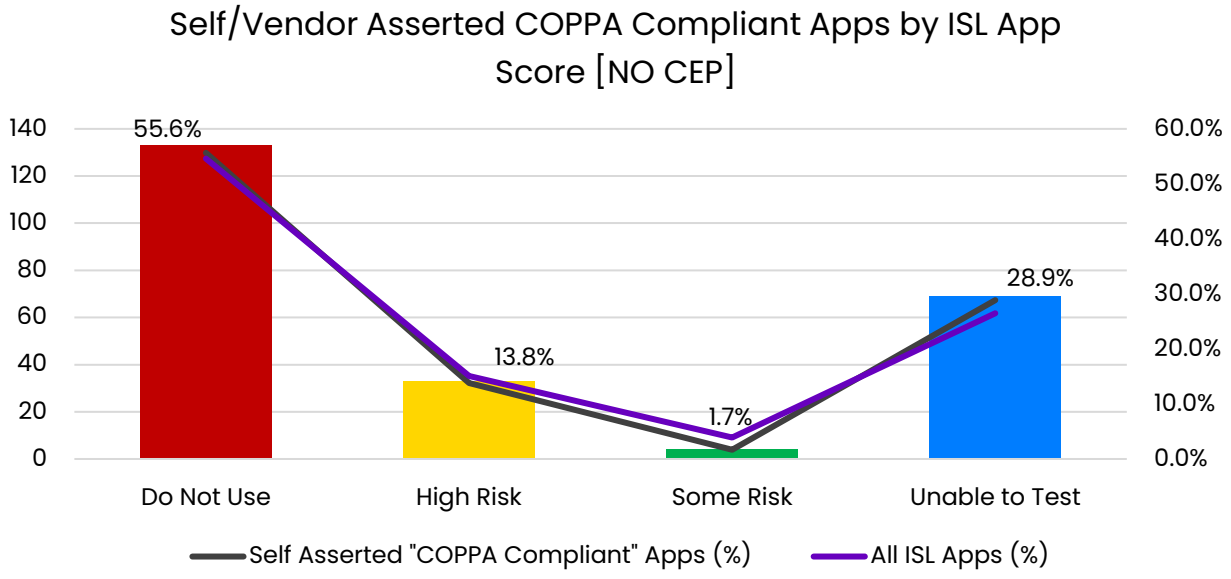


Figure 7.31b

7.4.1.2 Examination of Do Not Use Scores

With regard to the number of DNU criteria found in the self-asserted COPPA compliant apps, the apps that received DNU scores had a higher percent of only 1 Criteria compared to the overall data set (55.6% vs. 48.0%, Figure 7.32b)—a positive difference.

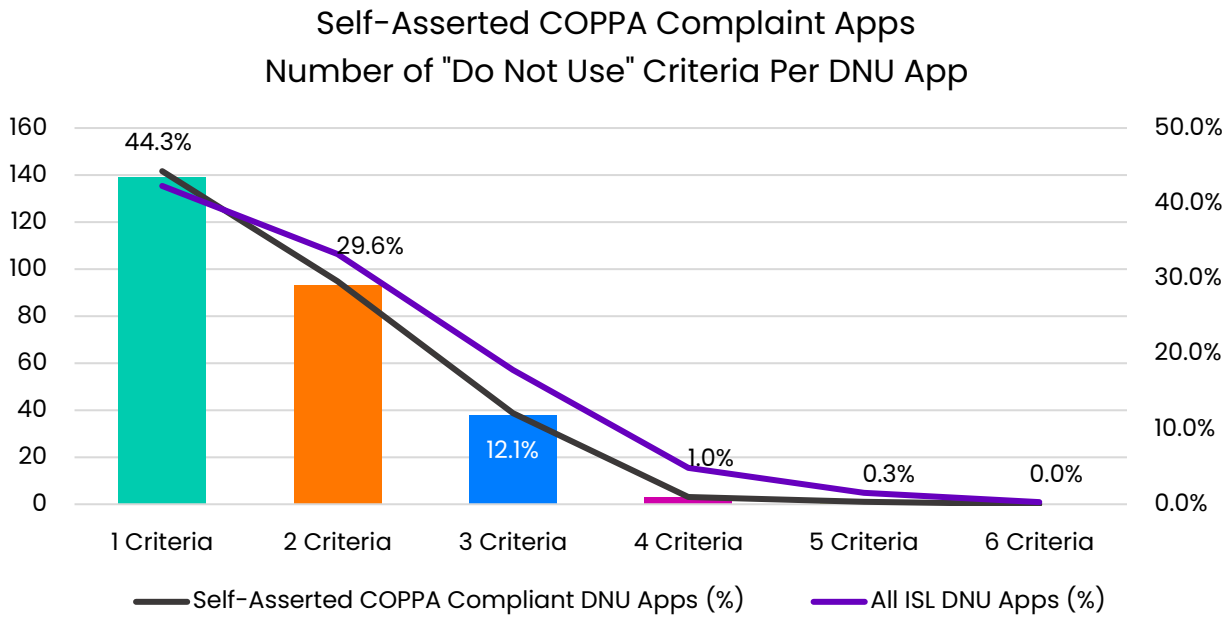


Figure 7.32a

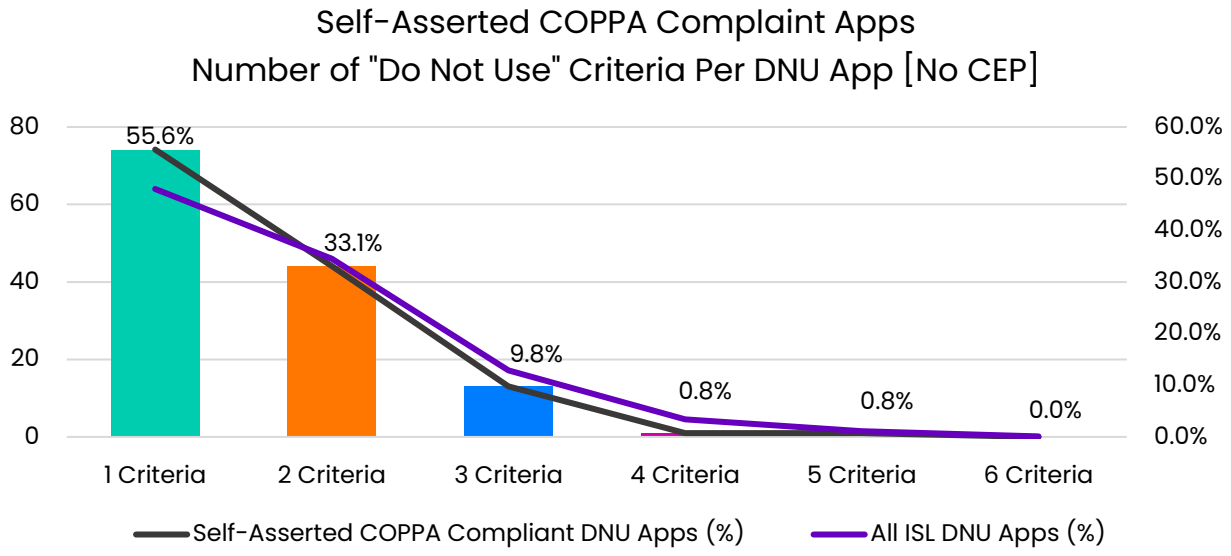


Figure 7.32b

The self-asserted COPPA compliant apps with DNU scores had a slightly higher percent of Adobe network traffic (4.5% vs. 2.5%) and a somewhat higher percent of Amazon network traffic (30.8% vs. 23.3%, Figure 7.33b).

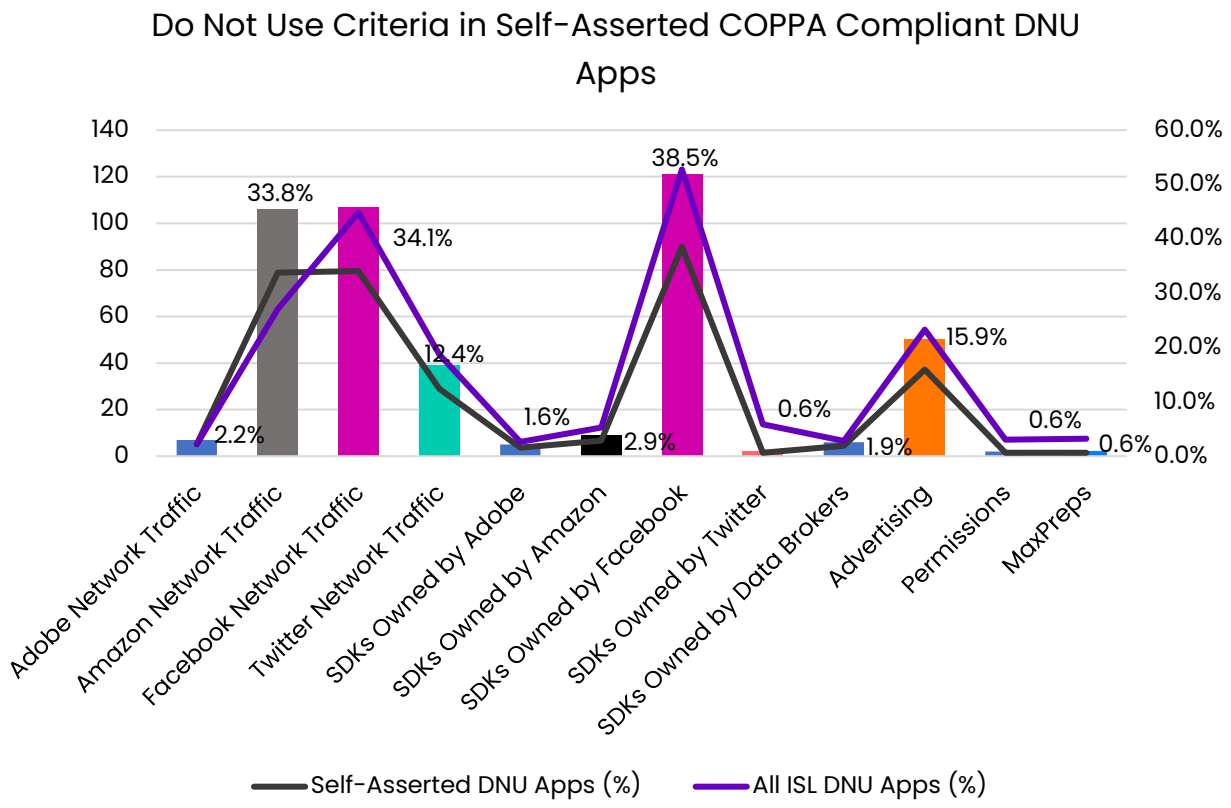


Figure 7.33a

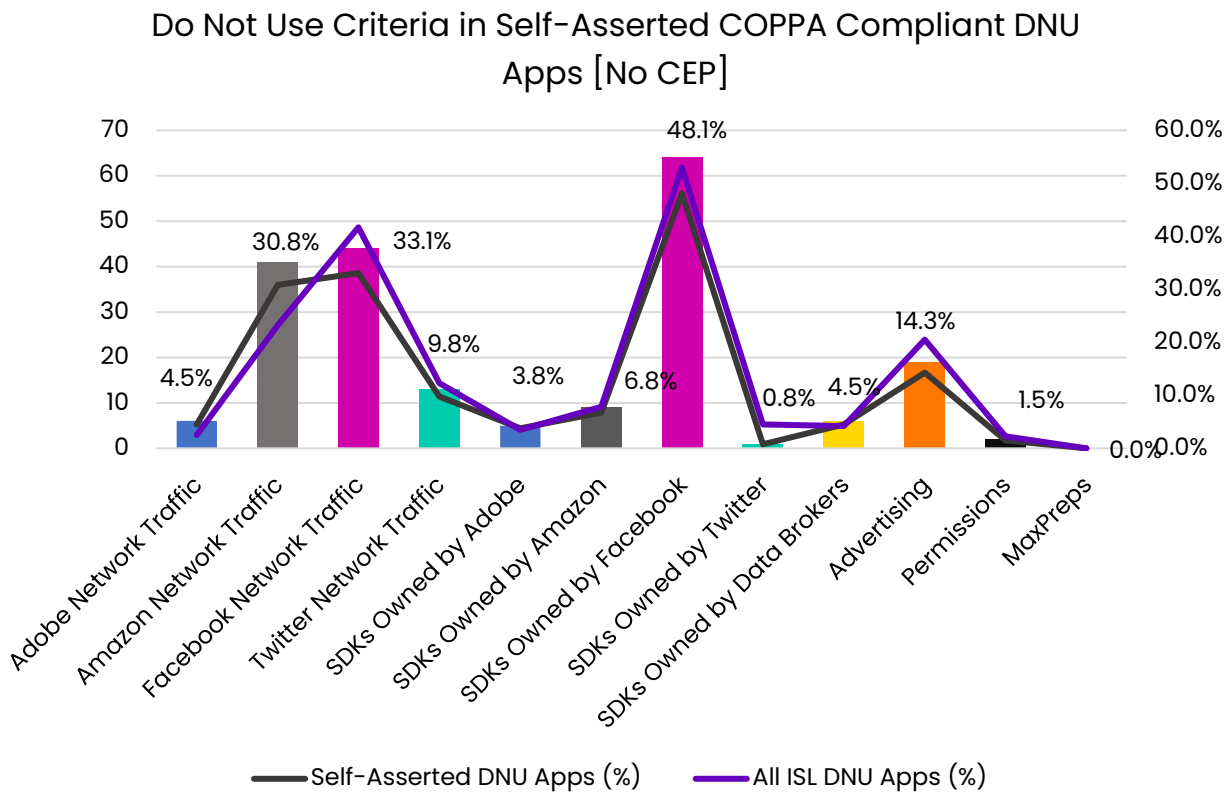


Figure 7.33b

7.4.1.3 Advertising Presence

The self-asserted COPPA compliant apps performed better than the overall sample set with respect to ads (11.2% vs. 15.2%) and retargeting ads (7.1% vs. 8.9%, Figure 7.34b).

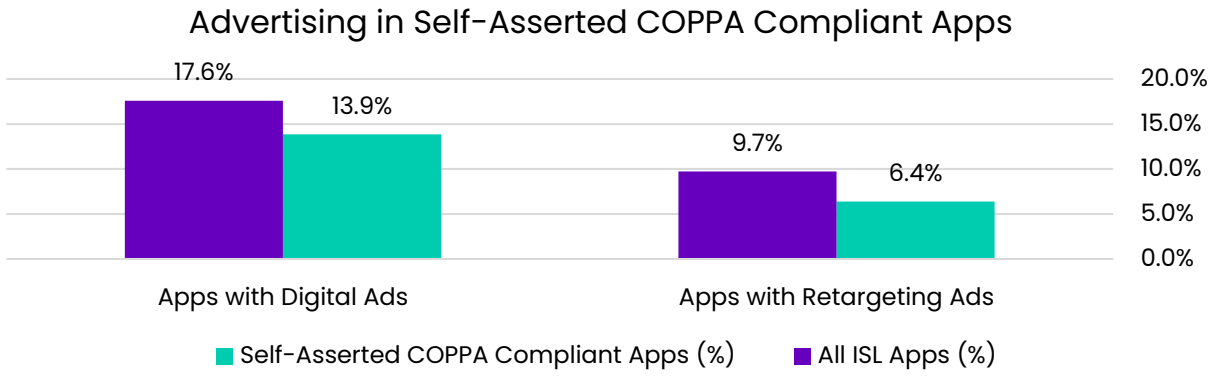


Figure 7.34a

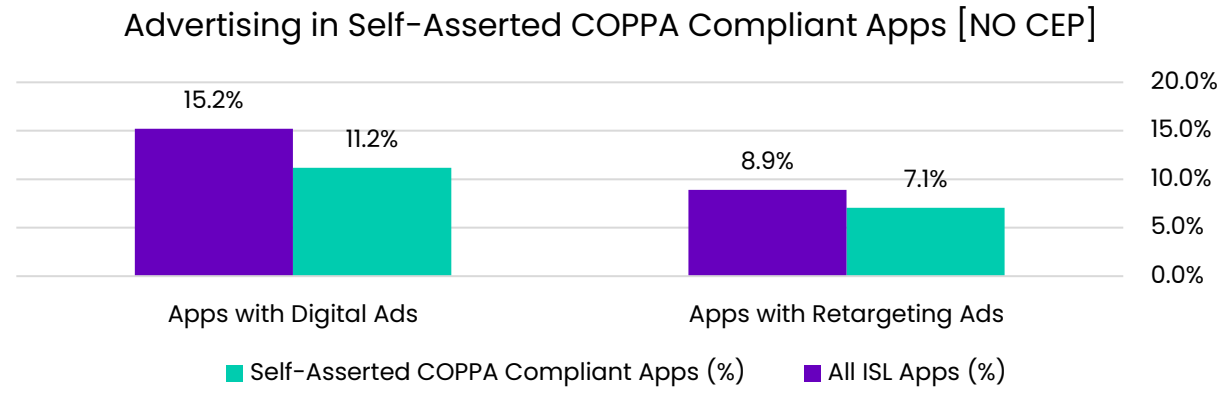


Figure 7.34b

7.4.1.4 Most Recommended Self-Asserted COPPA Compliant Apps

Figure 7.35 shows the most recommended apps with self-asserted COPPA compliance in the sample based on frequency of use across all schools in the sample.

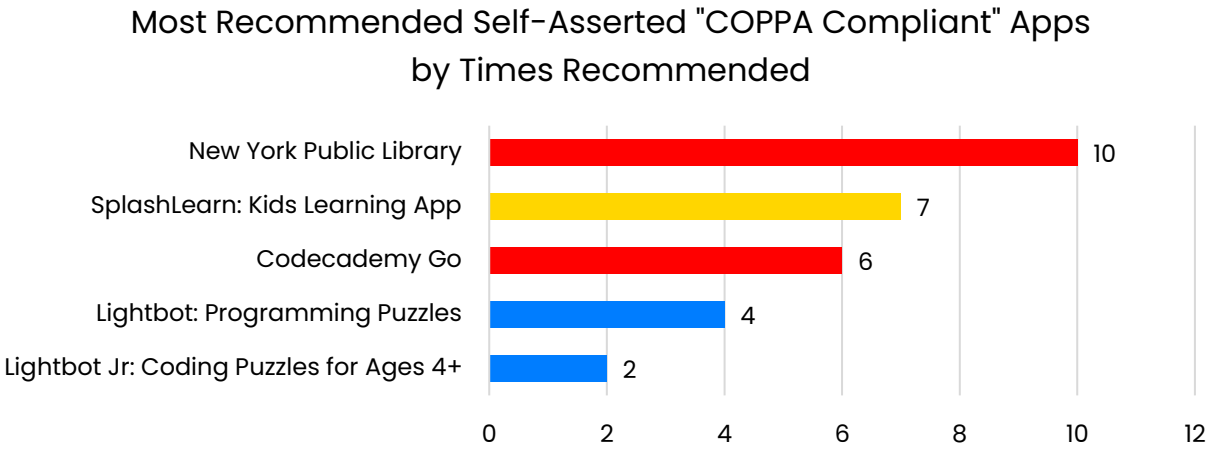


Figure 7.35

7.5 Student Privacy Pledge

The Student Privacy Pledge is an enforceable commitment that companies can voluntarily make. The pledge, in existence since 2014 and revised in 2020, is the product of the Future of Privacy Forum and the Software & Information Industry Association. EdTech Vendors can voluntarily make this public commitment to

safeguard student privacy and comply with the pledge commitments. The Student Privacy Pledge states that it's intended to align with general FERPA requirements and many state student privacy laws that also prohibit the sale of student PII.[xix]

The pledge is enforceable by the Federal Trade Commission under their Section 5 Authority of unfair or deceptive trade practices.

Understanding the Pledge's Prohibitions and Promises

The Student Privacy Pledge prohibits:

- Collecting, using, and sharing Student PI beyond what is needed for authorized educational purposes *unless it is authorized by parent/student.*
- Selling Student PII (Personally Identifiable Information)
- Personal profiles of students unless it is for authorized educational purposes or as authorized by parent/student.

Vendors who sign onto this pledge also promise to:

- provide clear disclosures in contracts or privacy policies
    - These disclosures should include the types of students PII is collected, purposes for which info maintained is used or shared with third parties
- support students with access and correction of Student PII

On its face, the prohibitions and promises in the pledge seem impactful, but there are some limitations with the Pledge.

The definition of "School Service Provider" refers to any entity that provides online products or services *that are designed and marketed for use in K12 educational institution/agencies* and used at the direction of their employees and that collect, maintain, or use student personally identifiable information (PII) in a digital format.

[xix] Notably, the Student Privacy Pledge clearly states that it is not a third-party audit.

The Pledge also expressly excludes entities that provide online products or services for a general audience (aka not *designed and marketed for use in K12 schools).* As explored in Findings Report 1, a sizable percentage of the apps analyzed in this benchmark were non-education specific, and not explicitly for use by children.

7.5.1 Findings

There were 321 apps whose creators signed Student Privacy Pledges in the sample set. Removing the CEP apps leaves 158 "pledging" apps. Apps with signed Student Privacy Pledges performed better than the overall sample on both ISL Safety Scores and the presence of advertising, including retargeting advertising.

7.5.1.1 App Scores

Apps that signed the pledge performed significantly better in the Do Not Use category at 38.6% compared to 54.6% in the overall sample set (Figure 7.36b).

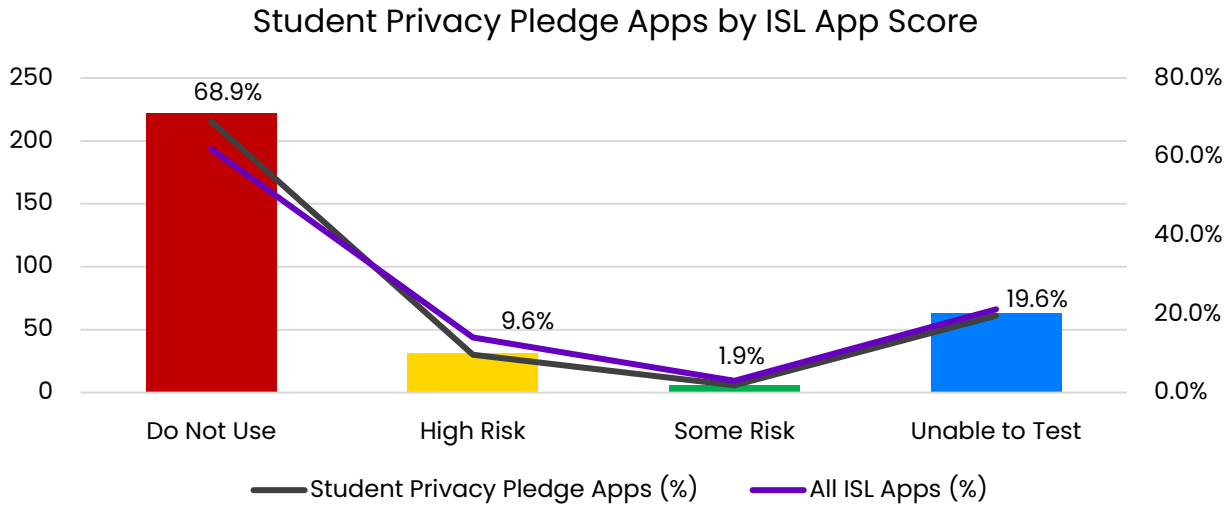


Figure 7.36a

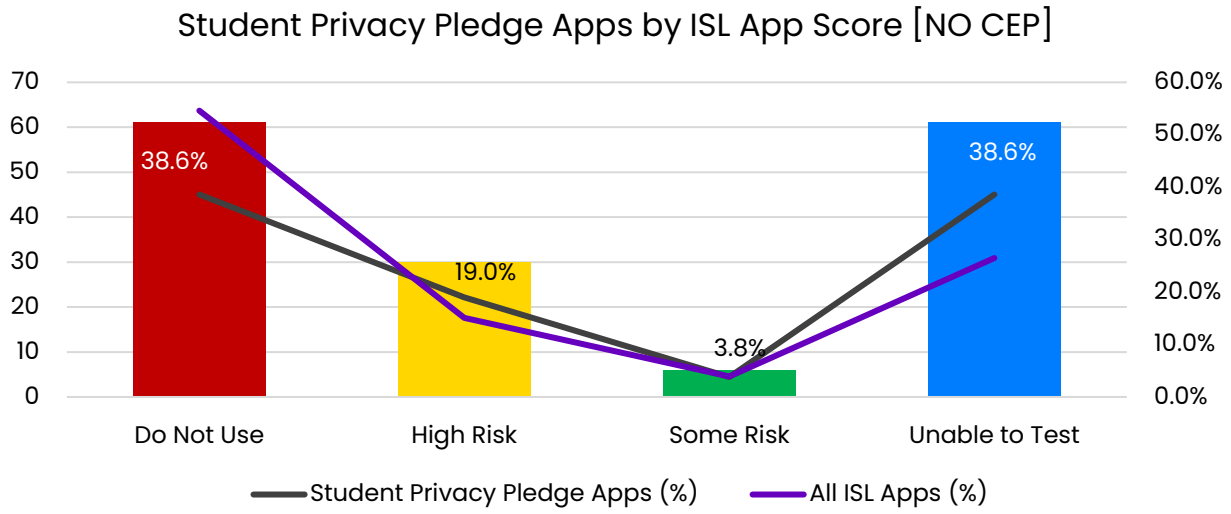


Figure 7.36b

7.5.1.2 Examination of Do Not Use Scores

One can see the distorting effect of the CEP apps in Figure 7.37a, where the Student Privacy Pledge apps that received a DNU score are more likely to have three and four Do Not Use criteria than the overall sample set. Removing the CEP apps results in a "healthier" distribution with 67.2% of the Student Privacy Pledge with DNU scores having only one DNU criteria (Figure 7.37b).

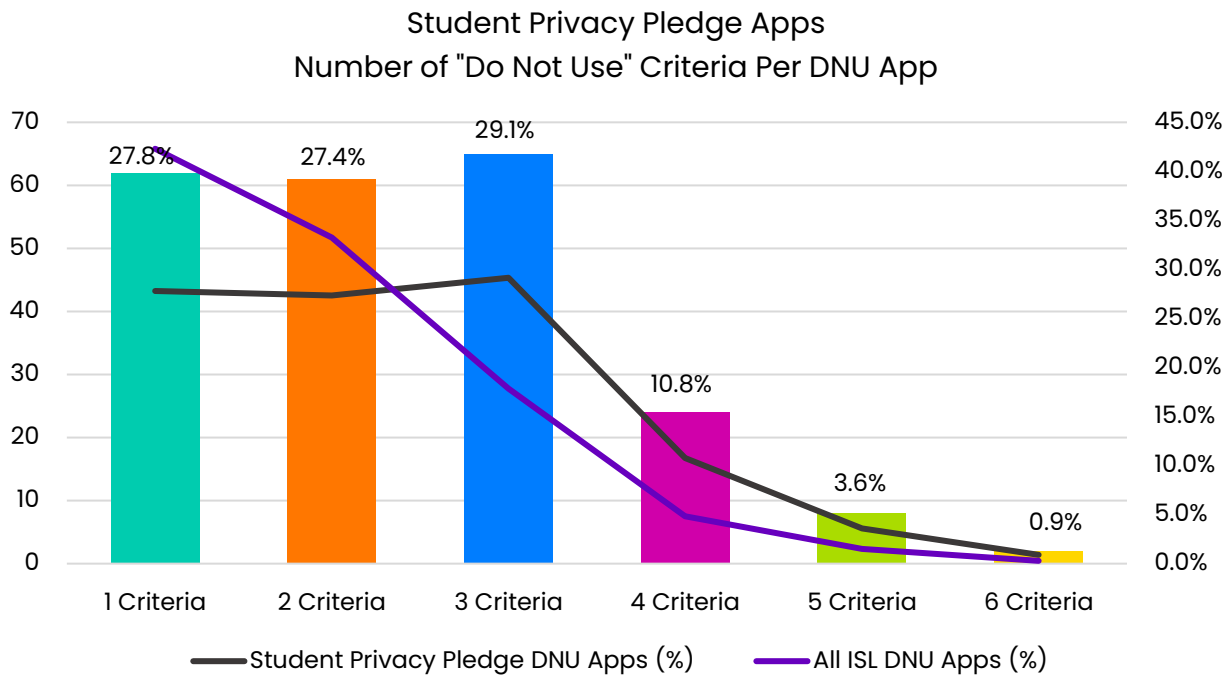


Figure 7.37a

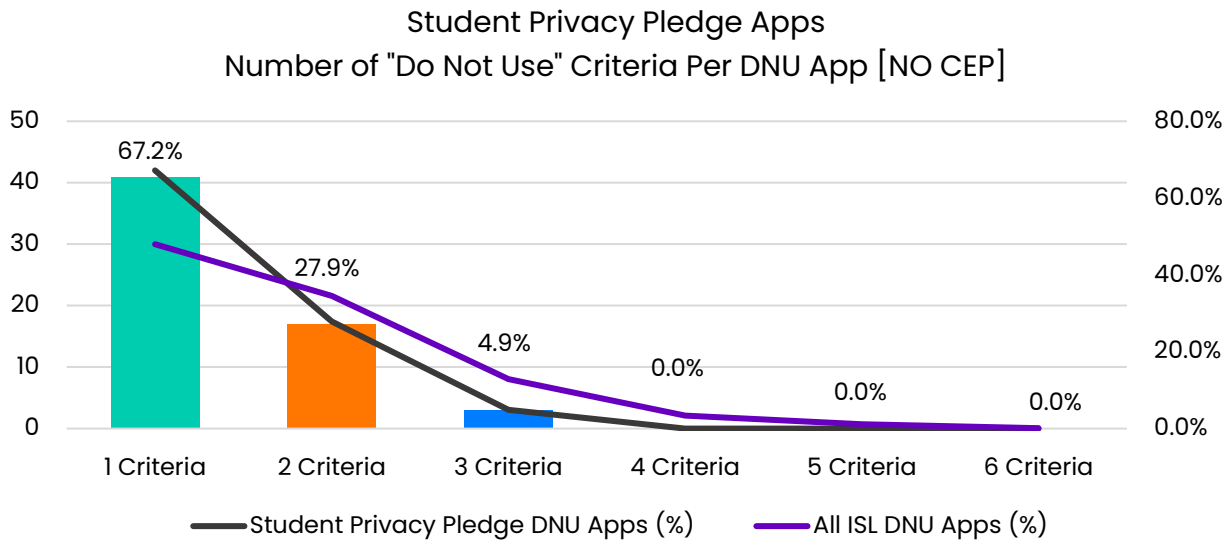


Figure 7.37b

Similarly, Figures 7.38a and 7.38b show the same distortion effect from the CEP apps. With the CEP apps, the Student Privacy Pledge apps that received a DNU score are more likely to send data to Facebook, Twitter, and Amazon, and more

likely to include Facebook and Twitter SDKs than the overall sample set (Figure 7.38a). The effect of MaxPreps is also clear—as it was only ever observed in the CEP apps. With the removal of the CEP apps (Figure 7.38b), the DNU triggers in the Student Privacy Pledge apps resembles the overall shape of total sample set, but with substantially lower percentages of Facebook network traffic, Facebook SDKs, and advertising triggers.

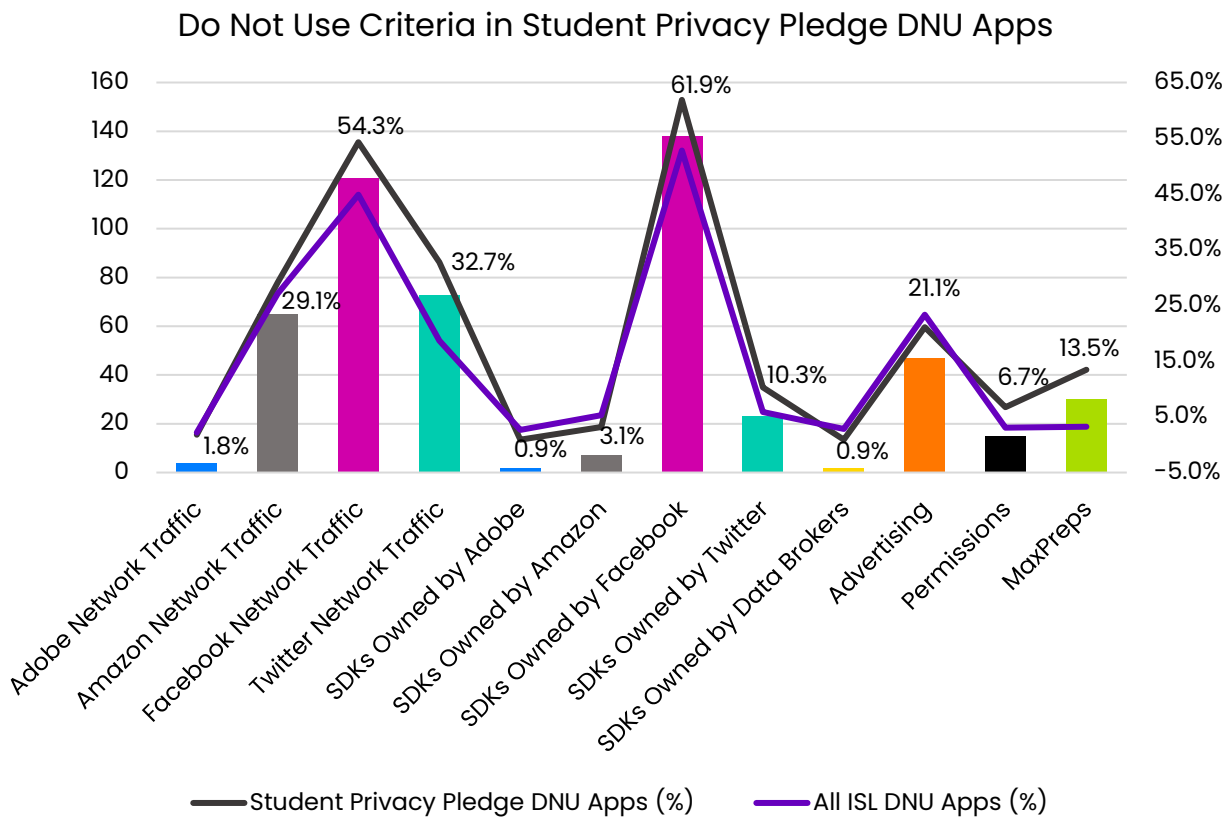


Figure 7.38a

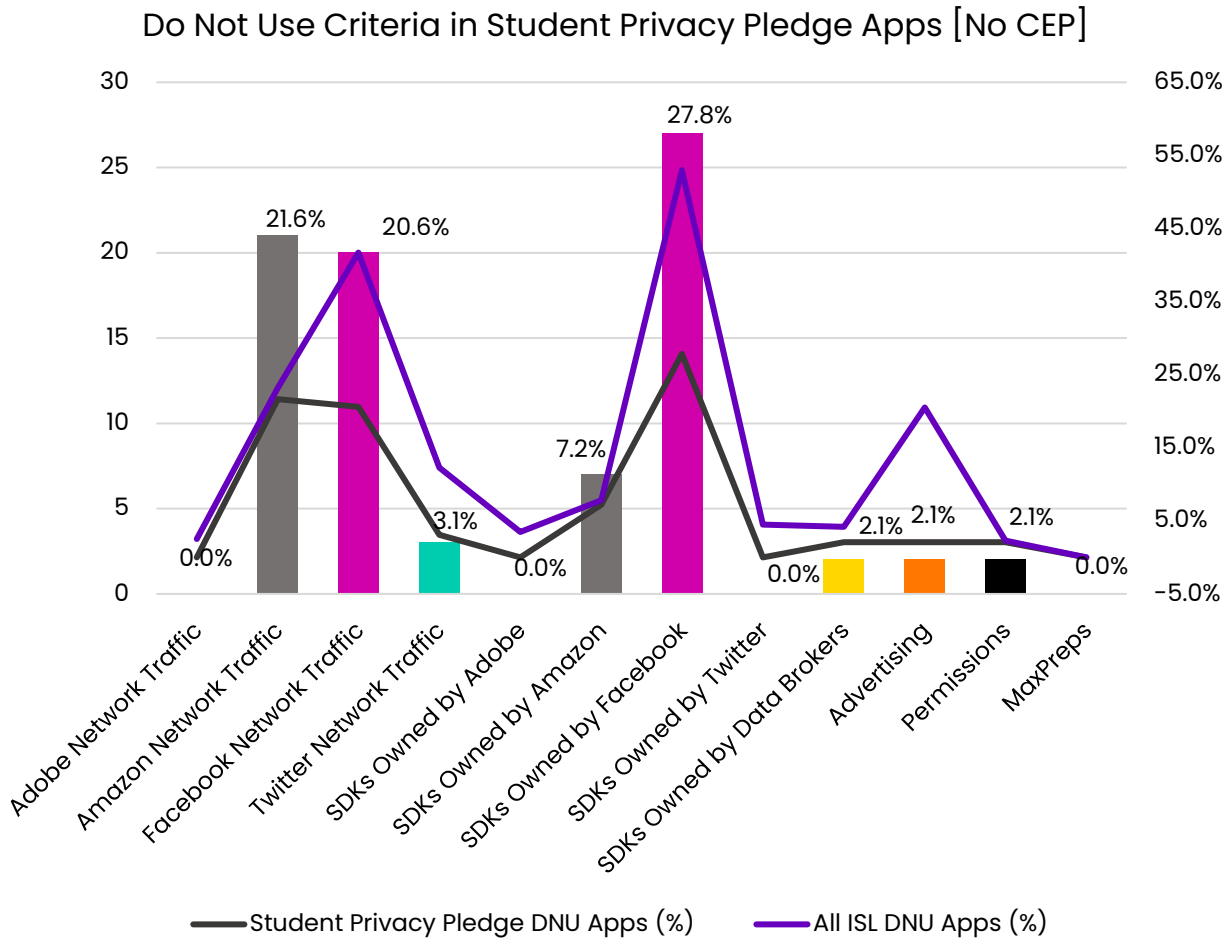


Figure 7.38b

7.5.1.3 Advertising Presence

The Student Privacy Pledge apps were much less likely to include both digital apps and retargeting apps than the overall sample set (Figure 7.39b). They also performed better than the set of apps with any certification or promise (of which 7.9% included ads).

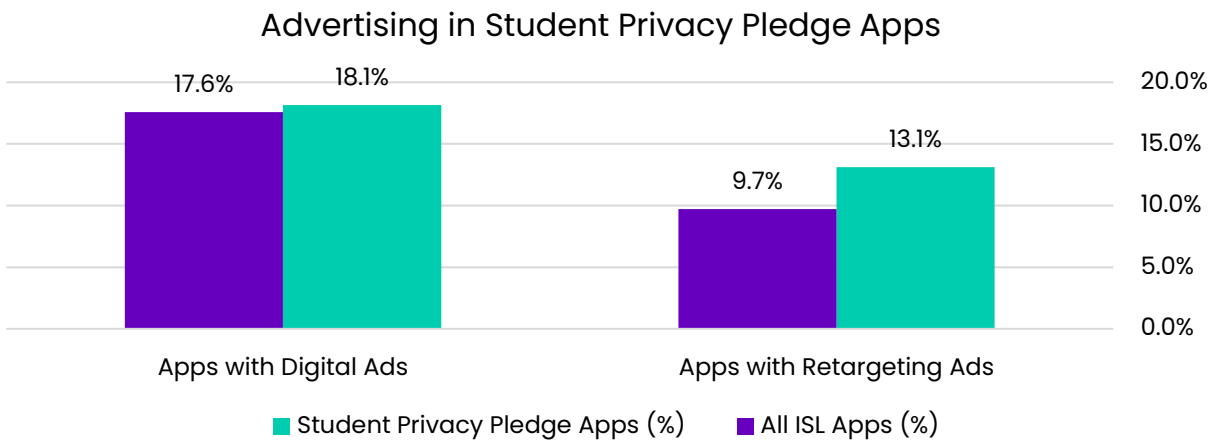


Figure 7.39a

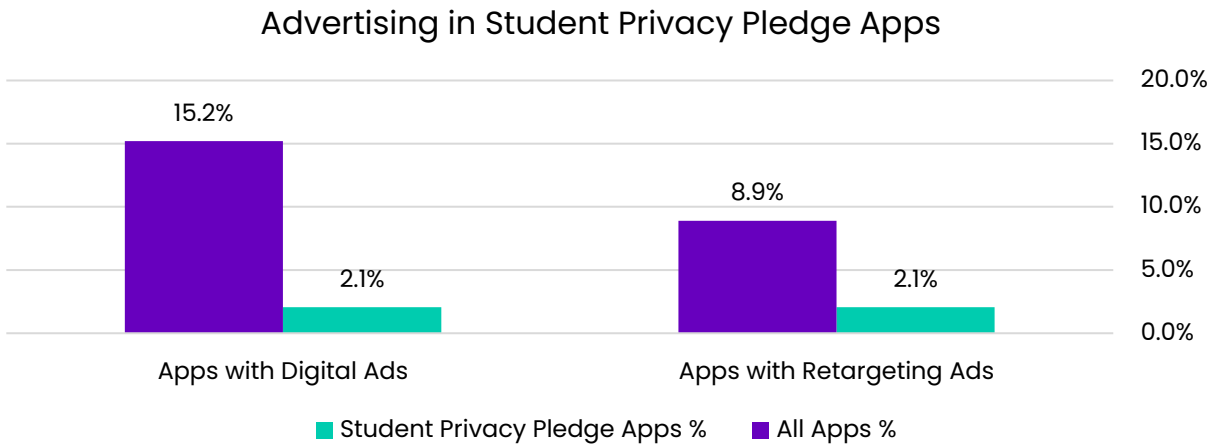


Figure 7.39b

7.5.1.4 Most Recommended Student Privacy Pledge Apps

Figure 7.40 shows the most recommended Student Privacy Pledge apps in the sample based on frequency of use across all schools in the sample.

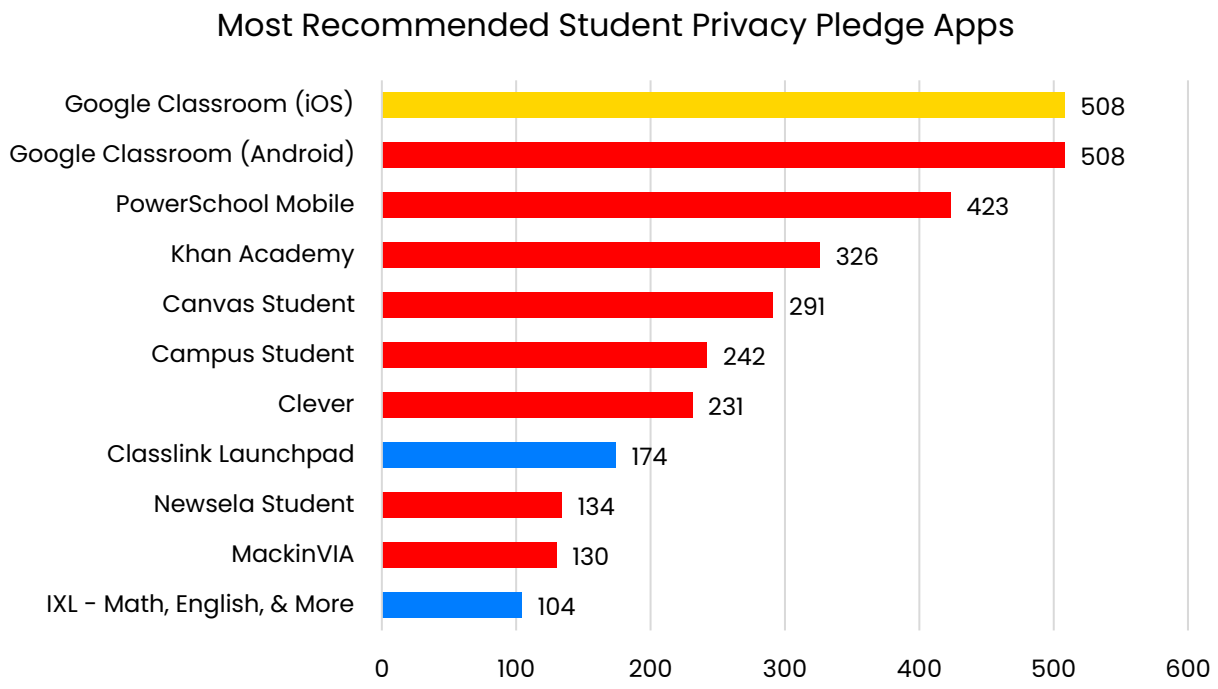


Figure 7.40

7.6 SDPC

SDPC is a global organization that facilitates various state alliances in the US, supporting LEAs and vendors by providing helpful resources and tools for the creation and management of data privacy agreements.

Thanks to the SDPC's work in creating the National Data Privacy Agreement (NDPA), LEAs can pro-actively assert privacy terms for student data.

SDPC's standard form data privacy agreement and publicly searchable database allow others to see which providers and LEAs have signed agreements within a particular state.

The standard format of the NDPA agreement makes the NDPA a better and easier choice for LEAs and tech providers alike because after both parties become familiar with the standard form and the requirements therein the parties can duplicate the process with other parties and devote their focus on the information included in Exhibits A, B, G, and H when contracting with different parties.

- **Exhibit A** provides a detailed description of the tech provider's products and services.
- **Exhibit B** provides checkboxes for the collected data points.
- **Exhibit G** incorporates and lists out state regulations, and contractually obligates the parties to recognize those laws.[xx]
- **Exhibit H** lists all the vendor specific and district edits. Any changes to the standard terms of the NDPA may be made/found on Exhibit G and H of the NDPA.

Moreover, states can and do create their own variants of Data Privacy Agreements to best align with state mandates.

Figure 7.41 below is a visual representation of SDPC's role in student data privacy. The SDPC facilitates the creation of boilerplate student data privacy agreements for use by schools and technology vendors. These agreements are signed by both the LEA and the technology vendor, likely in addition to an overall service agreement for the LEA's use of the technology.

[xx] According to the NDPA guidance docs, "Exhibit G terms should be limited to those mandated by specific laws or regulations. Exhibit G additions will supplement or replace the referenced standard NDPA clause(s)." https://cdn.ymaws.com/www.a4l.org/resource/resmgr/files/sdpc-publicdocs/SDPC_NDPA_Dev_Processes_2021.pdf

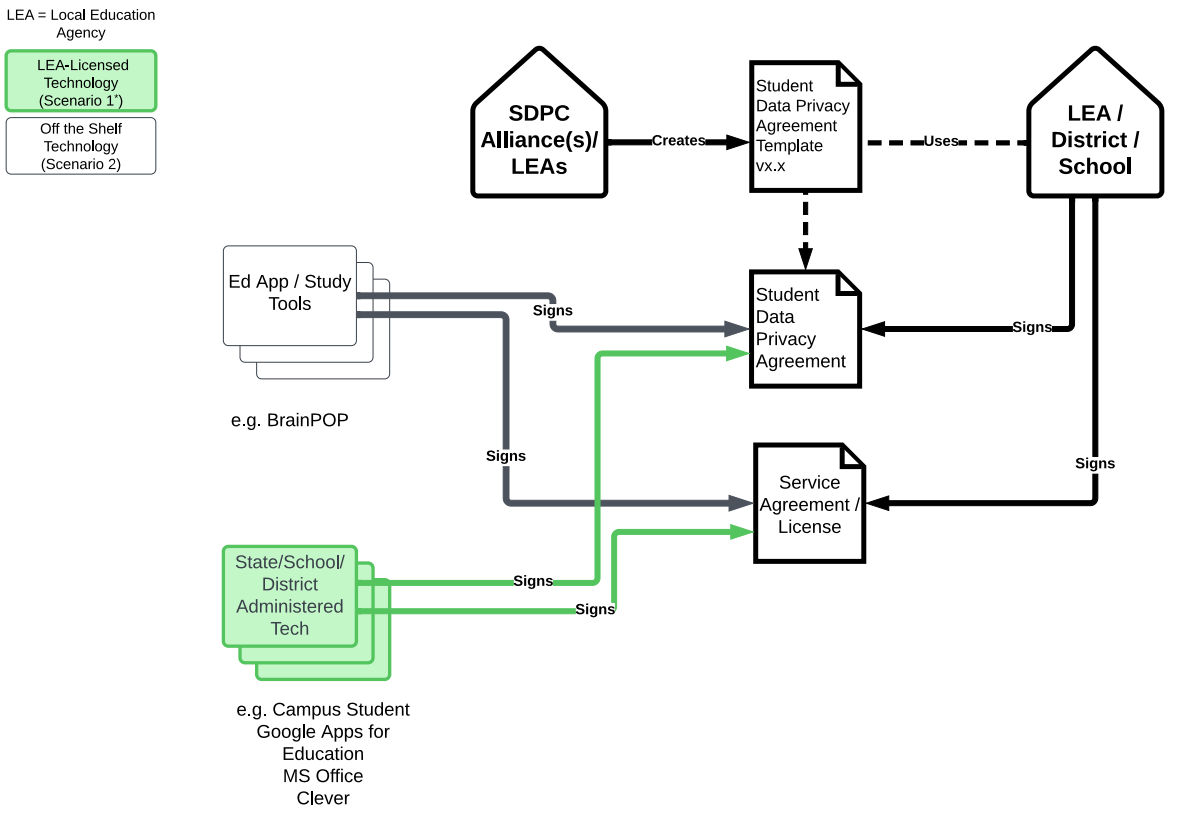


Figure 7.41

Observations

As noted earlier, SDPC doesn't appear to evaluate product behavior. The NDPA itself does not seem to incorporate any requirements to vet the actual product behavior.

Additionally, after reviewing a small sample size of NDPAs posted on SDPC's website, we noticed a common theme in EdTech Vendors responses when it comes to their detailed description of the products and services in Exhibit A. Some vendors may just point LEAs to their Terms of Service and Privacy Policy in Exhibit A. The full extent of what a vendor ultimately decided to provide in Exhibit A varied from a short and basic description of their services to no description of their

products and services at all other than a link to their Terms of Service and Privacy Policy.

7.6.1 Findings

There were 368 SDPC apps in the set of overall data set, of those, four were CEP apps, resulting in a total studied set of 364 apps.

7.6.1.1 App Scores

The SDPC apps behaved nearly identically to the overall data set with respect to the ISL Safety Score (Figure 7.42b).

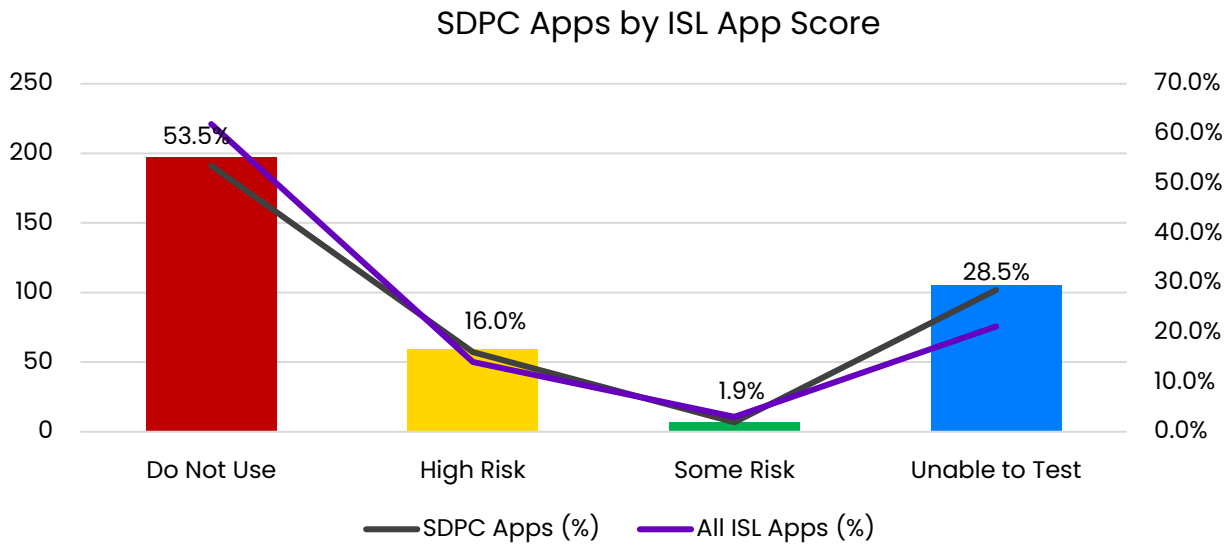


Figure 7.42a

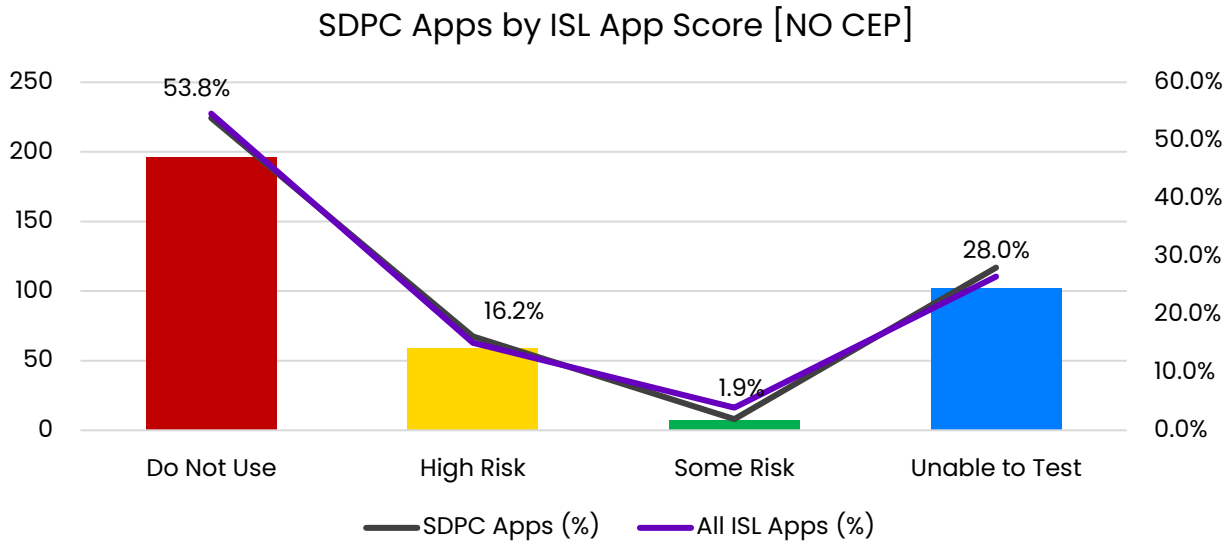


Figure 7.42b

7.6.1.2 Examination of Do Not Use Scores

Like the other certification and promise categories, the SDPC apps with DNU scores are "better" than the overall sample, with a higher percentage of apps with a single DNU criterion (56.6% vs 48.0%, Figure 7.43b).

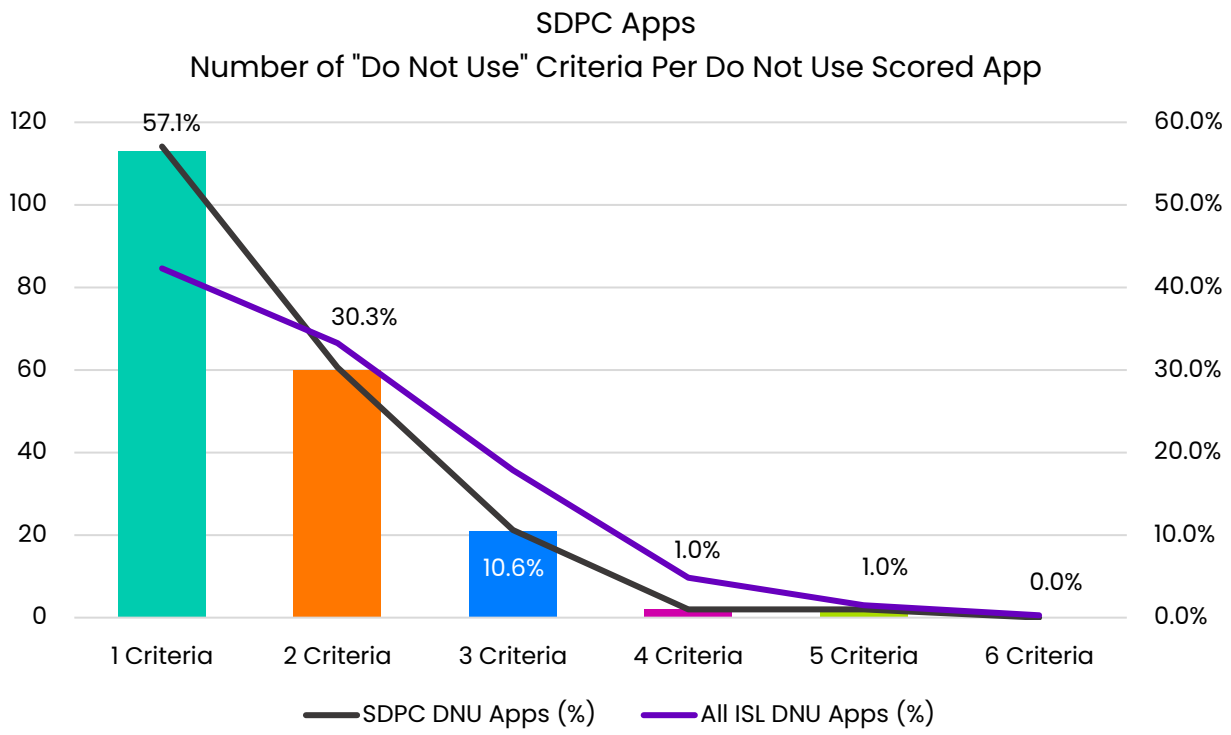


Figure 7.43a

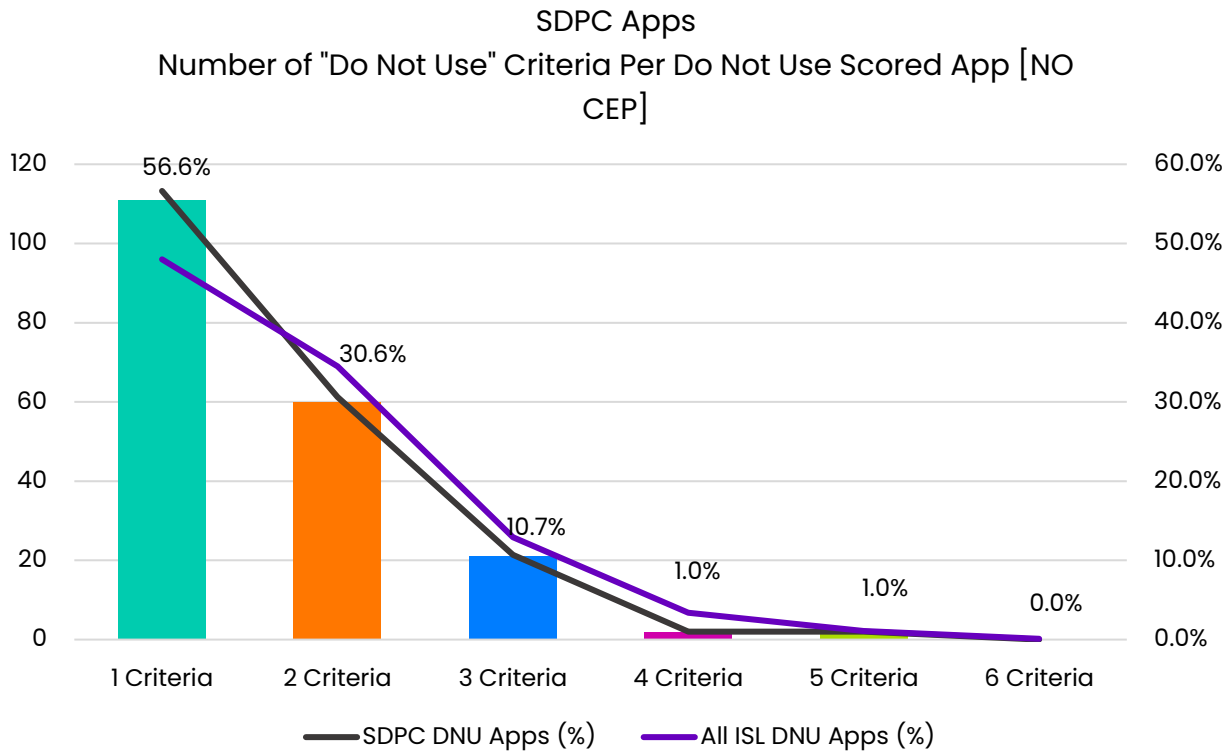


Figure 7.43b

The distribution of Do Not Use triggers mirrors the overall sample set nearly identically (Figure 7.44b) with the exception of advertising as a DNU trigger which is about half as likely in SDPC apps than in the overall sample set (10.7% vs. 20.5%).

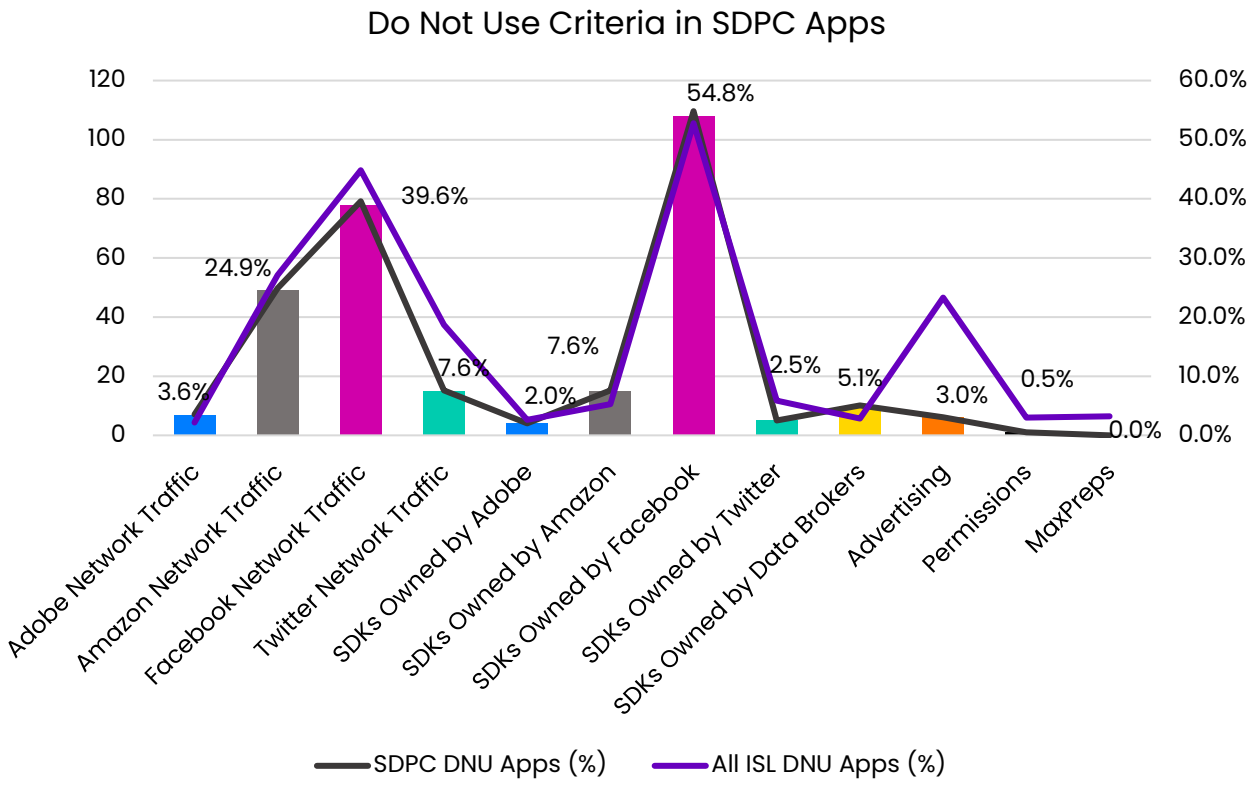


Figure 7.44a

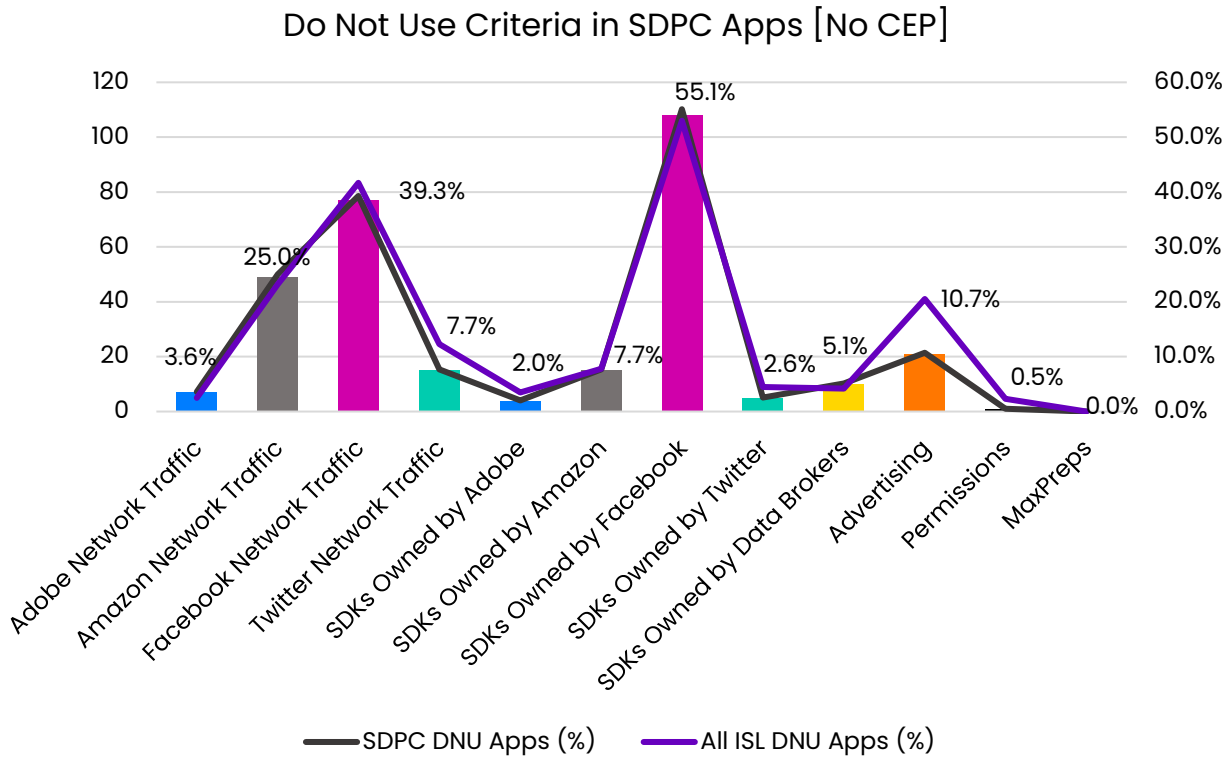


Figure 7.44b

7.6.1.3 Advertising Presence

SDPC apps had a significantly lower percentage of ads (8.0% vs 15.2%) and retargeting ads (2.3% vs 8.9%) than the overall dataset (Figure 7.45b).

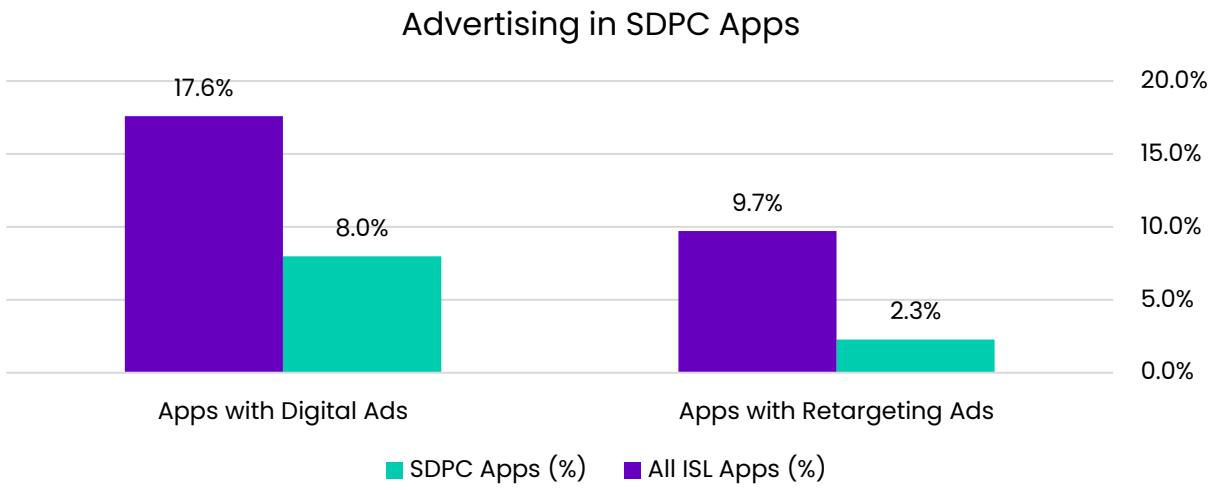


Figure 7.45a

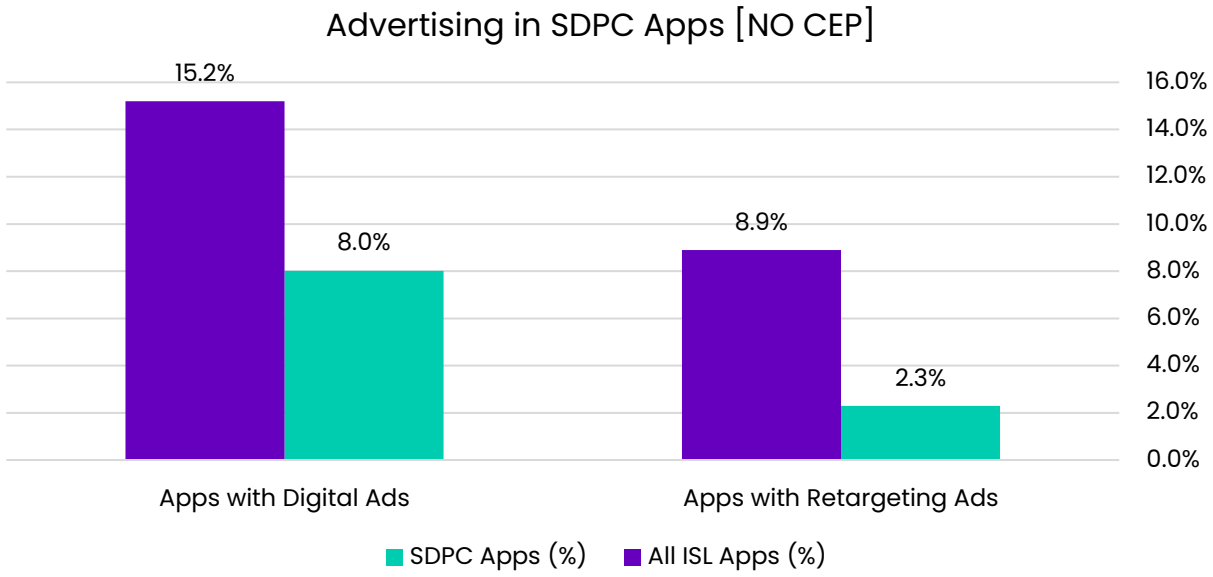


Figure 7.45b

7.6.1.4 Most Recommended SDPC Apps

Figure 7.46 shows the most recommended SDPC apps in the sample based on frequency of use across all schools in the sample.

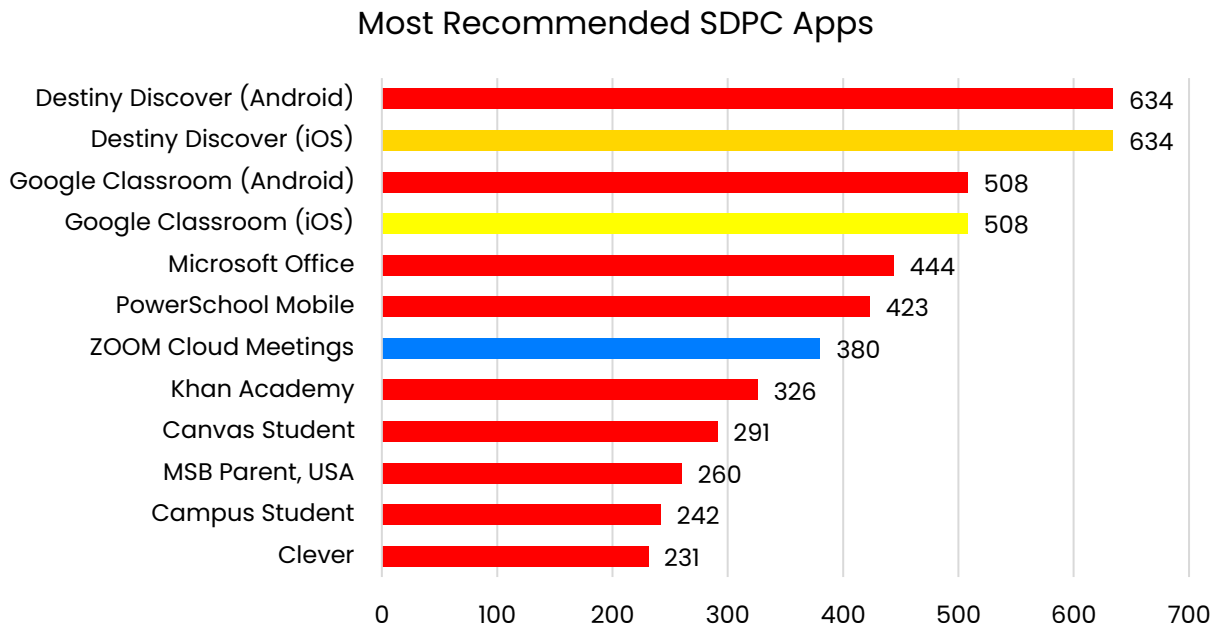


Figure 7.46

8 Recommendations

8.1 Best Practices for Schools/LEAs

8.1.1 Technology Notice and Consent in Schools

While notice and consent (also known as notice and choice) is the cornerstone of nearly all privacy regulation, it is surprisingly absent in student privacy regulation. ISL believes students and parents deserve to know exactly what technology is required and what is optional for students.

Recommendation 1:

Schools should provide easily accessible lists of all technology students will use for schoolwork, with clear indications of "mandatory" vs. "optional" for each listed technology.

ISL believes that the information should be easy for parents and students to find at any time. Ideally, this information should always be available on the school or district website and be accurate. The proposed solution here isn't to mandate behaviors through legislation, necessarily. This is something that schools and LEAs can effectively manage with some simple examples of best practices. Use of SDPC, for example, is a very straightforward and robust way for schools to publish technology notices.

Recommendation 2:

Even though it's not currently legally required in all cases, ISL believes that allowing parents and students to consent to mandatory technology is a best practice.

ISL further believes that students and parents should always have a choice and not be forced to use technology that puts students at risk. We realize that this can be difficult for schools, and the best way to ensure students aren't being subjected to potential harms through unsafe technology is to perform meaningful technology vetting.

8.1.1.1 Overuse of School Consent for Technology

Recommendation 3:

Schools/LEAs should only provide consent on behalf of the student for technologies that the school has a relationship with.

It's questionable if schools/LEAs *can* realistically consent on behalf of the student in cases where technology is used either without a login or with credentials obtained independently by the student or parent.

8.1.2 Technology Vetting

What's a school to do when certifications and privacy practices fail to stop the flow of student data to risky entities? Based on our research, current school vetting—and certification and promise practices—may not be as effective as needed.

Recommendation 4:

ISL recommends that schools have a systemic safety vetting practice for all technology required or recommended by the school.

Vetting must include at minimum, annual data supply auditing, akin to what ISL has done in this benchmark. It's not reasonable to expect schools or LEAs to perform this vetting with current resources. With the forthcoming launch of ISL's app safety labels, schools will be armed with considerable, accurate information about EdTech apps' data supply.

Additionally, 1EdTech certification and Data Privacy Agreements such as those facilitated by SDPC appear to be resulting in safer apps, so this is something that schools can do today.

8.2 Regulation Observations

8.2.1 COPPA Safe Harbor Certification

As can be seen from section 7.2, COPPA Safe Harbor certification appears to only be positively affecting the presence of retargeting advertising. While this is excellent news and possibly an indication that the certification is performing as the regulation is designed, ISL believes these certified apps have too much advertising, and are too frequently sharing student data with risky, large platforms like Facebook and Twitter. We realize that lawmakers recognize shortcomings of COPPA based on the COPPA revision initiatives in progress. We hope that the data

in this report sheds light on the risks still presented to students by technologies that they use.

8.2.2 Regulatory Exclusions for General Audience Services/Products

With nearly 30% of technology recommended in US schools being non-education specific, we suggest that SOPIPA and the Student Privacy Pledge be modified to include general audience services/products in privacy protections for students.

COPPA, however, appears to cover general audience services in the following way: COPPA EdTech providers can be regulated if the website or online service targets children as a primary or secondary audience, or is directed in whole or in part to children[xxi], or the company has actual knowledge that the user is a child under the age of 13, which Includes general audience websites and online services. ISL hopes that the raw data from our 2022 EdTech benchmark being released this year will be of service to the FTC and the COPPA Safe Harbor authorized entities.

[xxi] Including general audience websites with a section for children.

9 Appendix A: ISL Safety Score Rubric

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/
    - ISL researcher observed questionable permission behavior.
- **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 9.1 summarizes the ISL Safety Scoring rubric.

Table 9.1 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; 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	
		Questionable permission behavior.	

10 Appendix B: Community Engagement Platform (CEP) Apps in Benchmark

All CEP Apps							
State	**App Name**	**OS**	**# Down-loads**	**App Developer**	**Ads?**	**Retar-geting Ads?**	**App Score**
	Abeka Events	Android	1K-5K	Abeka	N	N	Do Not Use
	Abeka Events	iOS	N/A	Abeka	N	N	Do Not Use
NC	Alamance-Burlington Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
NC	Alamance-Burlington Schools	Android		Apptegy, Inc.	N	N	High Risk
PA	Albert Gallatin Area SD	Android	100-500	EMS LINQ, Inc.	--	--	Unable To Test
PA	Albert Gallatin Area SD	iOS	N/A	EMS LINQ, Inc.	--	--	Unable To Test
VA	Alexandria City Pub-lic Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
VA	Alexandria City Pub-lic Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
VA	Alleghany County Schools	Android	10-50	Intrado Corporation	N	N	Do Not Use
MT	Anaconda School District	Android	50-100	Apptegy, Inc.	N	N	High Risk
AK	Anchorage School District	Android	10K-50K	Blackboard	N	N	Do Not Use
AK	Anchorage School District	iOS	N/A	Blackboard	N	N	Do Not Use
TX	Anna Coyote Athlet-ics	Android	100-500	Mascot Media, LLC	Y	N	Do Not Use
TX	Anna Coyote Athlet-ics	iOS	N/A	Mascot Media, LLC	Y	N	Do Not Use
TX	Anna ISD	iOS	N/A	Blackboard	N	N	Do Not Use
DE	Appoquinimink School District	Android	1K-5K	Educational Net-works, Inc.	N	N	Do Not Use
DE	Appoquinimink School District	iOS	N/A	Educational Net-works, Inc.	N	N	Do Not Use
GA	Atlanta Public Schools (APS)	Android	1K-5K	Blackboard	Y	Y	Do Not Use
GA	Atlanta Public Schools (APS)	iOS	N/A	Blackboard	Y	Y	Do Not Use
CO	Aurora Public Schools	iOS	N/A	Neon Rain Interac-tive	--	--	Unable To Test
MD	Baltimore City Public Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
MD	Baltimore City Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
VA	Bedford County School District	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
VA	Bedford County School District	iOS	N/A	Intrado Corporation	N	N	Do Not Use

SD	Bennett County School District	Android	100-500	Apptegy, Inc.	Spon-sorships	N	Do Not Use
SD	Bennett County School District	iOS	N/A	Apptegy, Inc.	Spon-sorships	N	Do Not Use
WV	Berkeley County Schools (WV)	Android	10K-50K	Blackboard	Y	Y	Do Not Use
WV	Berkeley County Schools (WV)	iOS	N/A	Blackboard	Y	Y	Do Not Use
ME	Biddeford School District, ME	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
ME	Biddeford School District, ME	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AL	Birmingham City Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
AL	Birmingham City Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
KS	Blessed Sacrament	iOS	N/A	Solutio, Inc.	N	N	Do Not Use
KS	Blessed Sacrament - Wichita, K	Android	100-500	Solutio, Inc.	N	N	Do Not Use
KS	Blue Valley Schools KS	Android	500-1K	Blackboard	N	N	Do Not Use
KS	Blue Valley Schools KS	iOS	N/A	Blackboard	Y	Y	Do Not Use
KY	Boone County Schools	Android	1K-5K	SchoolPointe, Inc.	N	N	Do Not Use
KY	Boone County Schools	iOS	N/A	SchoolPointe, Inc.	N	N	Do Not Use
RI	Bristol Warren Re-gional SD	Android	100-500	Blackboard	N	N	Do Not Use
RI	Bristol Warren Re-gional SD	iOS	N/A	Blackboard	N	N	Do Not Use
GA	Bryan County Schools, GA	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
GA	Bryan County Schools, GA	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
OH	Buckeye Local JH/HS	Android	1K-5K	SchoolInfoApp, LLC	Y	N	Do Not Use
OH	Buckeye Local School District	iOS	N/A	SchoolInfoApp, LLC	Y	N	Do Not Use
NC	Buncombe County Schools, NC	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
NC	Buncombe County Schools, NC	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
KS	Burlington Schools	Android	1K-5K	Gabbart Communi-cations	N	N	Do Not Use
KS	Burlington Schools	iOS	N/A	Gabbart Communi-cations	N	N	Do Not Use
DE	Caesar Rodney School District	iOS	N/A	Blackboard	N	N	Do Not Use
DE	Caesar Rodney School District	Android	N/A	Blackboard	N	N	Do Not Use
IA	Camanche Commu-nity School	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
IA	Camanche Commu-nity School	Android	100-500	Apptegy, Inc.	N	N	High Risk

MA	Cambridge Public Schools	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
MA	Cambridge Public Schools	iOS	N/A	Intrado Corporation	N	N	Do Not Use
GA	Carroll County School System	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
OK	Cascia Hall Prepara-tory School	Android	100-500	Straxis LLC	N	N	Do Not Use
OK	Cascia Hall Prepara-tory School	iOS	N/A	Straxis LLC	N	N	Do Not Use
IL	CCSD15	Android	1K-5K	Blackboard	N	N	Do Not Use
IL	CCSD15	iOS	N/A	Blackboard	N	N	Do Not Use
LA	CCSS Wildcats	Android	N/A	Apptegy, Inc.	N	N	High Risk
LA	CCSS Wildcats	iOS	N/A	Apptegy, Inc.	N	N	High Risk
NV	Centennial High School	iOS	N/A	Eldio, LLC	N	N	Do Not Use
NV	Centennial High School	Android	500-1K	Eldio, LLC	N	N	High Risk
NM	Central Consolidated Schools	iOS	N/A	Eldio, LLC	--	--	Unable To Test
NM	Central Consolidated Schools	Android	1K-5K	Eldio, LLC	--	--	Unable To Test
PA	Central Dauphin Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
PA	Central Dauphin Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
SD	Chamberlain School District	Android	100-500	Apptegy, Inc.	Y	N	Do Not Use
SD	Chamberlain School District	iOS	N/A	Apptegy, Inc.	Y	N	Do Not Use
SC	Charleston County Schools, SC	Android	1K-5K	Blackboard	N	N	Do Not Use
SC	Charleston County Schools, SC	iOS	N/A	Blackboard	N	N	Do Not Use
DE	Christina School Dis-trict	Android	1K-5K	Blackboard	N	N	Do Not Use
DE	Christina School Dis-trict	iOS	N/A	Blackboard	N	N	Do Not Use
WY	Cody Public Schools - Park 6	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WY	Cody Public Schools - Park 6	Android	500-1K	Apptegy, Inc.	N	N	High Risk
OK	Collinsville Public Schools	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
OK	Collinsville Public Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
TN	Columbia Academy Sports	Android	100-500	BallFrog.com, LLC	Y	N	Do Not Use
TN	Columbia Academy Sports	iOS	N/A	BallFrog.com, LLC	--	--	Do Not Use
TX	Comal ISD	Android	5K-10K	Blackboard	N	N	Do Not Use
TX	Comal ISD	iOS	N/A	Blackboard	N	N	Do Not Use
NC	Commmunityvisual	Android	10-50	Educational Net-works, Inc.	N	N	Do Not Use

MT	Corvallis MT School Dist	Android	100-500	Apptegy, Inc.	N	N	High Risk
MT	Corvallis MT School Dist	iOS	N/A	Apptegy, Inc.	N	N	High Risk
NJ	Cresskill Public Schools	Android	50-100	Apptegy, Inc.	N	N	Do Not Use
NJ	Cresskill Public Schools	iOS	N/A	Apptegy, Inc.	N	N	High Risk
WI	D.C. Everest School District	Android	500-1K	Blackboard	N	N	Do Not Use
WI	D.C. Everest School District	iOS	N/A	Blackboard	N	N	Do Not Use
NY	D29 Shines	Android	50-100	Solved Educational Consultancy, LLC	N	N	Do Not Use
FL	Dadeschools Mobile	Android	100K-500K	Miami-Dade County Public Schools	--	--	Do Not Use
FL	Dadeschools Mobile	iOS	N/A	Miami-Dade County Public Schools	--	--	Do Not Use
NE	DC West Community Schools	Android	100-500	Filament Essential Services	Y	N	Do Not Use
NE	DC West Community Schools	iOS	N/A	Filament Essential Services	Y	N	Do Not Use
MN	Deer River Schools ISD	Android	100-500	Blackboard	N	N	Do Not Use
AZ	Deer Valley Unified SD	Android	1K-5K	Blackboard	N	N	Do Not Use
AZ	Deer Valley Unified SD	iOS	N/A	Blackboard	N	N	Do Not Use
OK	Dickson Public Schools	iOS	N/A	Intrado Corporation	N	N	High Risk
KS	Dodge City Public Schools	Android	500-1K	Gabbart Communi-cations	N	N	Do Not Use
KS	Dodge City Public Schools	iOS	N/A	Gabbart Communi-cations	N	N	Do Not Use
CO	Dolores School Dis-trict	Android	100	Bluetree Apps	N	N	Do Not Use
CO	Dolores School Dis-trict	iOS	N/A	Bluetree Apps	N	N	Do Not Use
CO	Douglas County SD	Android	1K - 5K	Intrado Corporation	Y	N	Do Not Use
CO	Douglas County SD	iOS	N/A	Custom School Apps	Y	N	Do Not Use
FL	Duval County Public Schools	Android	10K-50K	Blackboard	N	N	Do Not Use
FL	Duval County Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
IN	East Allen County Schools	Android	1K-5K	Apptegy, Inc.	Y	N	Do Not Use
IN	East Allen County Schools	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
OH	East Cleveland City Schools	Android	100-500	Blackboard	--	--	Unable To Test
IN	East Noble	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
IN	East Noble	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
LA	EBR School System	Android	1K-5K	SchoolInfoApp, LLC	Y	N	Do Not Use
LA	EBR School System	iOS	N/A	SchoolInfoApp, LLC	Y	N	Do Not Use

OH	Edgewood City Schools, OH	Android	1K-5K	Apptegy, Inc.	Y	N	Do Not Use
	Edlio Engage	iOS	N/A	LivingTree	--	--	Unable to Test
ME	Ellsworth School Department	Android	10-50	Apptegy, Inc.	N	N	Do Not Use
ME	Ellsworth School Department ME	iOS	N/A	Apptegy, Inc.	N	N	High Risk
VT	Essex Westford School District	Android	100-500	Blackboard	N	N	Do Not Use
VT	Essex Westford School District	iOS	N/A	Blackboard	N	N	Do Not Use
IL	Essexville-Hampton Schools	Android	50-100	Apptegy, Inc.	N	N	Do Not Use
AR	eStem Public Charter Schools	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
AR	eStem Public Charter Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
GA	Floyd Co Schools	Android	10-50	Blackboard	N	N	Do Not Use
GA	Floyd Co Schools	iOS	N/A	Blackboard	N	N	Do Not Use
AR	Forrest City Mustangs	Android	100-500	Gabbart Communications	N	N	Do Not Use
AR	Fort Smith PS Athletics	Android	50-100	Mascot Media, LLC	Y	N	Do Not Use
AR	Fort Smith PS Athletics	iOS	N/A	Mascot Media, LLC	Y	Y	Do Not Use
KY	Garrard County Schools, KY	Android	N/A	Apptegy, Inc.	N	N	Do Not Use
KY	Garrard County Schools, KY	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
MI	Gladstone Area Schools	Android	100-500	Intrado Corporation	N	N	Do Not Use
ND	Grand Forks 1 School District	iOS	N/A	Blackboard	N	N	Do Not Use
ND	Grand Forks Public Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
NE	Grand Island PS	Android	1K-5K	Edulink Systems, Inc.	N	N	Do Not Use
NE	Grand Island PS	iOS	N/A	Edulink Systems, Inc.	N	N	High Risk
NE	Grand Island Public Schools	Android	100-500	Intrado Corporation	N	N	Do Not Use
SC	Greenville County Schools	Android	5K-10K	Intrado Corporation	Y	N	Do Not Use
AZ	GUSD1	Android	100-500	Apptegy, Inc.	N	N	High Risk
AZ	GUSD1	iOS	N/A	Apptegy, Inc.	N	N	High Risk
AL	Haleyville City Schools	Android	50-100	Apptegy, Inc.	N	N	Do Not Use
AL	Haleyville City Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
NY	Hamburg CSD	Android	100-500	Intrado Corporation	N	N	Do Not Use
NY	Hamburg CSD	iOS	N/A	Intrado Corporation	N	N	Do Not Use
TN	Hamilton County Schools	Android	1K-5K	Intrado Corporation	--	--	Do Not Use

WV	Hancock County Schools, WV	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
WV	Hancock County Schools, WV	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Harrison County Schools, WV	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
WV	Harrison County Schools, WV	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AL	Hartselle City Schools	Android	500-1K	Blackboard	N	N	Do Not Use
AL	Hartselle City Schools	iOS	N/A	Blackboard	N	N	Do Not Use
TX	Hays CISD	Android	5K-10K	Blackboard	Y	Y	Do Not Use
TX	Hays CISD	iOS	N/A	Blackboard	Y	Y	Do Not Use
KS	Hays USD 489, KS	Android	100-500	Apptegy, Inc.	Y	Y	Do Not Use
KS	Hays USD 489, KS	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
MD	HCPSS	Android	10K-50K	Intrado Corporation	N	N	Do Not Use
MD	HCPSS	iOS	N/A	Intrado Corporation	N	N	Do Not Use
GA	Henry County Schools (GA)	Android	500-1K	Blackboard	Y	Y	Do Not Use
KS	Hesston Swathers	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
KS	Hesston Swathers	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
TX	Holy Family Catholic School TX	Android	10-50	Aware3, LLC	--	--	Do Not Use
TX	Holy Family Catholic School TX	iOS	N/A	Aware3, LLC	--	--	Do Not Use
OH	Hudson City Schools - OH	Android	1K-5K	Blackboard	Y	Y	Do Not Use
OH	Hudson City Schools - OH	iOS	N/A	Blackboard	Y	Y	Do Not Use
NY	Hudson Falls CSD	Android	N/A	Intrado Corporation	N	N	Do Not Use
NY	Hudson Falls CSD	iOS	500-1k	Intrado Corporation	N	N	Do Not Use
NV	Humboldt County Schools, NV	Android	100-500	Apptegy, Inc.	N	N	High Risk
TX	Iola Independent School Distri	Android	100-500	Blackboard	N	N	Do Not Use
MS	Jackson Public Schools - MS	Android	1K-5K	Blackboard	N	N	Do Not Use
MS	Jackson Public Schools - MS	iOS	N/A	Blackboard	N	N	Do Not Use
AR	Jacksonville North Pulaski, AR	Android	500-1K	Apptegy, Inc.	Y	N	Do Not Use
AR	Jacksonville North Pulaski, AR	iOS	N/A	Apptegy, Inc.	Y	N	Do Not Use
AR	Jacksonville Titans Athletics	Android	50-100	Mascot Media, LLC	Y	N	Do Not Use
AR	Jacksonville Titans Athletics	iOS	N/A	Mascot Media, LLC	Y	N	Do Not Use
ND	Jamestown 1-ND	Android	1K-5K	Blackboard	Y	Y	Do Not Use
ND	Jamestown 1-ND	iOS	N/A	Blackboard	Y	N	Do Not Use
KY	JCPS	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
KY	JCPS	iOS	N/A	Intrado Corporation	N	N	Do Not Use

UT	JE Cosgriff Memorial School	iOS	N/A	Aware3, LLC	N	N	Do Not Use
UT	JE Cosgriff Memorial School	Android	10-50	Aware3, LLC	N	N	High Risk
AL	Jefferson County SD	Android	100-500	Blackboard	N	N	Do Not Use
AL	Jefferson County SD	iOS	N/A	Blackboard	N	N	Do Not Use
KS	Jefferson West USD 340	Android	100-500	Apptegy, Inc.	Y	Y	Do Not Use
KS	Jefferson West USD 340	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
KY	Johnson County Schools	Android	500-1K	Apptegy, Inc.	N	N	Do Not Use
KY	Johnson County Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
IA	Johnston Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
IA	Johnston Schools	iOS	N/A	Blackboard	N	N	Do Not Use
AK	Kenai Peninsula Borough SD	Android	1K-5K	Blackboard	N	N	Do Not Use
AK	Kenai Peninsula Borough SD	iOS	N/A	Blackboard	N	N	Do Not Use
KY	Kenton County School District	iOS	N/A	SchoolPointe, Inc.	N	N	Do Not Use
KY	Kenton County School District	Android	1K-5K	SchoolPointe, Inc.	N	N	High Risk
WI	Kewaskum School District	Android	100-500	SchoolPointe, Inc.	N	N	Do Not Use
WI	Kewaskum School District	iOS	N/A	SchoolPointe, Inc.	--	--	Do Not Use
KY	KHSAA/Riherds Scoreboard	iOS	N/A	Frank Riherd	Y	Y	Do Not Use
TX	La Feria ISD	Android	500-1K	Intrado Corporation	Y	N	Do Not Use
WY	Laramie 1 Safe	Android	50-100	CutCom Software Inc	N	N	High Risk
WY	Laramie 1 Safe	iOS	N/A	CutCom Software Inc	N	N	High Risk
WY	LCSD 1	iOS	N/A	Gabbart Communications	N	N	Do Not Use
KS	Leavenworth USD 453	Android		Blackboard	Y	N	Do Not Use
KS	Leavenworth USD 453	iOS	N/A	Blackboard	Y	N	Do Not Use
CO	Lewis-Palmer SD #38	Android	500-1K	Blackboard	Y	N	Do Not Use
CO	Lewis-Palmer SD #38	IOS	N/A	Blackboard	Y	N	Do Not Use
WY	Lincoln County School District	Android	50-100	Gabbart Communications	N	N	Do Not Use
RI	Lincoln Public Schools	Android	5-10	Blackboard	N	N	Do Not Use
RI	Lincoln Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
AR	Little Rock School District	Android	1K-5K	Blackboard	Y	N	Do Not Use
AR	Little Rock School District	iOS	N/A	Blackboard	Y	N	Do Not Use

MS	Madison County Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
MS	Madison County Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
MT	Malta Public Schools	Android	50-100	Apptegy, Inc.	N	N	Do Not Use
MT	Malta Public Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
TX	Mansfield ISD Athletics	Android	100-500	Mascot Media, LLC	Y	N	Do Not Use
TX	Mansfield ISD Athletics	iOS	N/A	Mascot Media, LLC	Y	N	Do Not Use
TX	Mansfield Tiger SuperFan	iOS	N/A	SuperFanU, Inc.	--	--	Do Not Use
VT	Maple Run Unified School, VT	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
VT	Maple Run Unified School, VT	iOS	N/A	Apptegy, Inc.	N	N	Some Risk
ME	Maranacook Area Schools	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
ME	Maranacook Area Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Marion County Schools, WV	Android	500-1K	Apptegy, Inc.	N	N	Do Not Use
WV	Marion County Schools, WV	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
KY	Marshall County Schools	Android	1K-5K	SchoolPointe, Inc.	--	--	Unable To Test
KY	Marshall County Schools	iOS	N/A	SchoolPointe, Inc.	--	--	Unable To Test
MO	Marshall Public Schools, MO	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
MO	Marshall Public Schools, MO	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
AK	Matanuska-Susitna Borough SD	Android	1K-5K	Blackboard	N	N	Do Not Use
AK	Matanuska-Susitna Borough SD	iOS	N/A	Blackboard	N	N	Do Not Use
AR	Mayflower School District, AR	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
AR	Mayflower School District, AR	iOS	N/A	Apptegy, Inc.	N	N	High Risk
ND	McKenzie County School Dist.	Android	500-1K	Blackboard	N	N	Do Not Use
ND	McKenzie County School Dist.	iOS	N/A	Blackboard	N	N	Do Not Use
NH	Merrimack School District	Android	500-1k	Intrado Corporation	N	N	Do Not Use
NH	Merrimack SD	iOS	N/A	Intrado Corporation	N	N	Do Not Use
TN	Metro Nashville Public Schools	Android	100-500	Intrado Corporation	N	N	Do Not Use
TN	Metro Nashville Public Schools	iOS	N/A	Intrado Corporation	N	N	Do Not Use
TX	Midland ISD	Android	1K-5K	Blackboard	N	N	Do Not Use
TX	Midland ISD	iOS	N/A	Blackboard	N	N	Do Not Use
	Minga	Android	10K-50K	Minga	--	--	Unable to Test

	Minga	iOS	N/A	Minga	--	--	Unable to Test
MO	Monroe City R1 School District	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
MO	Monroe City R1 School District	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
MD	Montgomery Public Schools	Android	10K-50K	Blackboard	Y	Y	Do Not Use
WV	Morgan County Schools, WV	Android	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Morgan County Schools, WV	iOS	100-500	Apptegy, Inc.	N	N	Do Not Use
MI	Mount Clemens Community School	Android	50-100	Appazur Solutions Inc.	N	N	Do Not Use
MI	Mount Clemens Community School	iOS	N/A	Appazur Solutions Inc.	N	N	Do Not Use
ME	MSAD #1	Android	N/A	Apptegy, Inc.	N	N	Do Not Use
ME	MSAD #1	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
GA	Murray County Schools	Android	1K-5K	SchoolInfoApp, LLC	N	N	Do Not Use
GA	Murray County Schools	iOS	N/A	SchoolInfoApp, LLC	N	N	Do Not Use
OK	Mustang Bands	Android	50-100	Karpster LLC	--	--	Unable To Test
OK	Mustang Bands	iOS	N/A	Karpster LLC	--	--	Unable To Test
UT	myDSD	Android	10K-50K	Davis School District	--	--	Do Not Use
FL	MySDMC Focus	Android	5K-10K	Focus School Software LLC	N	N	Do Not Use
FL	MySDMC Focus	iOS	N/A	Focus School Software LLC	N	N	Do Not Use
MN	MySPPS Saint Paul Public Schoo	Android	5K-10K	Blackboard	N	N	Do Not Use
MN	MySPPS St Paul Schools	iOS	N/A	Blackboard	N	N	Do Not Use
ID	Nampa Christian Schools	Android	100-500	Aware3, LLC	N	N	Do Not Use
ID	Nampa Christian Schools	iOS	N/A	Aware3, LLC	N	N	Do Not Use
	Nearpod	iOS	N/A	Nearpod, Inc.	--	--	Do Not Use
	Nearpod	Android	1M-5M	Nearpod, Inc.	--	--	Unable to Test
GA	New Creation Christian Academy	iOS	N/A	Aware3, LLC	N	N	Do Not Use
CT	New Fairfield Public Schools	Android	50-100	Apptegy, Inc.	N	N	High Risk
CT	New Haven Public Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
CT	Newtown Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
NY	NYC District 31 Staten Island	Android	100-500	Solved Educational Consultancy, LLC	N	N	Do Not Use
NY	NYC District 31 Staten Island	iOS	N/A	Solved Educational Consultancy, LLC	N	N	High Risk

NY	NYC Queens District 29 Shines	iOS	N/A	Solved Educational Consultancy, LLC	N	N	High Risk
ND	Oakes Public Schools	Android	500-1K	Blackboard	Y	Y	Do Not Use
ND	Oakes Public Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
MA	O'Bryant School	Android	50-100	Educational Networks, Inc.	N	N	Do Not Use
MA	O'Bryant School	iOS	N/A	Educational Networks, Inc.	N	N	High Risk
FL	OCPS	Android	10K-50K	Intrado Corporation	Y	Y	Do Not Use
FL	OCPS	iOS	N/A	Intrado Corporation	Y	Y	Do Not Use
WV	OH County Schools, WV	Android	100-500	Apptegy, Inc.	Y	Y	Do Not Use
WV	OH County Schools, WV	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
KS	Olathe Public Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
KS	Olathe Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
NC	Onslow County Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
OK	Oologah-Talala Public Schools	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
OK	Oologah-Talala Public Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
LA	Ouachita Parish Schools	Android	500-1K	Gabbart Communications	N	N	Do Not Use
LA	Ouachita Parish Schools	iOS	N/A	Gabbart Communications	N	N	Do Not Use
FL	Palm Beach County School Dist	Android	10K-50K	Intrado Corporation	Y	Y	Do Not Use
FL	Palm Beach County School Dist	iOS	N/A	Intrado Corporation	Y	Y	Do Not Use
FL	Palm Beach County SIS Gateway	Android	5K-10K	Focus School Software LLC	Y	N	Do Not Use
FL	Palm Beach County SIS Gateway	iOS	N/A	Focus School Software LLC	N	N	Do Not Use
LA	Parkway High School	Android	500-1K	SchoolInfoApp, LLC	Y	N	Do Not Use
LA	Parkway High School	iOS	N/A	SchoolInfoApp, LLC	Y	N	Do Not Use
WV	PCS Connect	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
WV	PCS Connect	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AL	Pell City Schools	Android	100-500	Blackboard	N	N	Do Not Use
AL	Pell City Schools	iOS	N/A	Blackboard	N	N	Do Not Use
PA	Phoenixville Area SD	Android	100-500	Intrado Corporation	Y	N	Do Not Use
IL	Pikeland CUSD #10, IL	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
IL	Pikeland CUSD #10, IL	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
FL	Plant City High School	Android	1K-5K	Heather Hanks	Y	Y	Do Not Use
FL	Plant City HS	iOS	N/A	Heather Hanks	Y	Y	Do Not Use
MO	Portageville School District	iOS	N/A	Intrado Corporation	N	N	Do Not Use

MD	Prince George's County PS	Android	10K-50K	Blackboard	Y	Y	Do Not Use
MD	Prince George's County PS	iOS	N/A	Blackboard	Y	Y	Do Not Use
	Project Lead The Way	Android	1K-5K	Aventri, Inc.	--	--	Unable to Test
RI	Providence Schools	Android	100-500	Blackboard	Y	Y	Do Not Use
NY	PSAL - NYC	iOS	500-1k	NY City Department of Education	N	N	Do Not Use
NY	PSAL - NYC	Android	N/A	NY City Department of Education	N	N	High Risk
AR	Pulaski County SSD, AR	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
AR	Pulaski County SSD, AR	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
NE	Raymond Central Public Schools	iOS	N/A	Filament Essential Services	N	N	Do Not Use
NE	Raymond Central Public Schools	Android	N/A	Filament Essential Services	--	--	Unable To Test
DE	Red Clay CSD	Android	500-1K	Blackboard	N	N	Do Not Use
KY	Red Oak ISD	Android	1K-5K	Blackboard	N	N	Do Not Use
KY	Red Oak ISD	iOS	N/A	Blackboard	N	N	Do Not Use
SC	Richland One	Android	1K-5K	Blackboard	N	N	Do Not Use
SC	Richland One	iOS	N/A	Blackboard	N	N	Do Not Use
CA	Rincon Valley USD, CA	Android	500-1K	Apptegy, Inc.	N	N	High Risk
NM	Rio Rancho Public Schools, NM	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
NM	RioRancho Public Schools, NM	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
MO	Ritenour Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
MO	Ritenour Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
AR	Rogers Public Schools - AR	Android	1K-5K	Blackboard	Y	N	Do Not Use
AR	Rogers Public Schools - AR	iOS	N/A	Blackboard	N	N	Do Not Use
AR	Rogers Public Schools Athletics	Android	N/A	Mascot Media, LLC	Y	N	Do Not Use
NM	Roswell Independent Schools	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
NM	Roswell Independent Schools	iOS	N/A	Intrado Corporation	N	N	Do Not Use
AR	RPS Athletics	iOS	N/A	Mascot Media, LLC	Y	N	Do Not Use
ND	Rugby Public Schools	Android	100-500	Blackboard	N	N	Do Not Use
ND	Rugby Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
WA	San Juan Island SD	Android	100-500	Blackboard	N	N	Do Not Use
WA	San Juan Island SD	iOS	N/A	Blackboard	N	N	Do Not Use
CO	Sanford School District	IOS	N/a	Apptegy, Inc.	N	N	Do Not Use
CO	Sanford School District, CO	Android	100-500	Apptegy, Inc.	N	N	Do Not Use

NH	SAU 54 Rochester, NH	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
NH	SAU 54 Rochester, NH	iOS	N/A	Apptegy, Inc.	N	N	High Risk
	School Dismissal Manager	Android	10K-50K	School Dismissal Manager	--	--	Unable to Test
	School Dismissal Manager (SDM)	iOS	N/A	School Dismissal Manager	--	--	Unable to Test
WI	School District of Bloomer	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
WI	School District of Bloomer	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
MA	Scituate Public Schools	iOS	N/A	Scituate Public Schools, MA	N	N	High Risk
IN	Scott County School District 2	Android	100-500	Intrado Corporation	N	N	Do Not Use
VA	Scott County VA Schools	Android	10-50	Intrado Corporation	N	N	Do Not Use
TN	Sevier County School System	Android	1K-5K	Blackboard	N	N	Do Not Use
TN	Sevier County School System	iOS	N/A	Blackboard	N	N	Do Not Use
SD	Sioux Falls Schools	Android	500-1K	Apptegy, Inc.	N	N	Do Not Use
SD	Sioux Falls Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
OK	Skiatook Public Schools	Android	500-1K	Filament Essential Services	N	N	Do Not Use
UT	Skyline High School - UT	iOS	N/A	SchoolInfoApp, LLC	N	N	Do Not Use
UT	Skyline High School - UT	Android	500-1K	SchoolInfoApp, LLC	N	N	High Risk
DE	Smyrna School District	Android	500-1K	Intrado Corporation	N	N	Do Not Use
WV	Summers County Schools	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
WV	Summers County Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
OK	Tecumseh Public Schools	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
OK	Tecumseh Public Schools, OK	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AR	The New School App	iOS	N/A	Finalsite	N	N	Do Not Use
AR	The New School App	Android	100-500	Finalsite	N	N	High Risk
ID	The Village Charter School	Android	50-100	Apptegy, Inc.	N	N	Do Not Use
ID	The Village Charter School	iOS	N/A	Apptegy, Inc.	N	N	High Risk
OK	Thomas Fay Custer Schools	Android	N/A	Gabbart Communications	N	N	Do Not Use
OK	Thomas Fay Custer Schools	iOS	N/A	Gabbart Communications	N	N	Do Not Use
NJ	Tinton Falls School District	Android	N/A	Apptegy, Inc.	N	N	Do Not Use
NJ	Tinton Falls School District	iOS	N/A	Apptegy, Inc.	N	N	High Risk
VA	Titans Athletics	Android	100-500	From Now On, LLC	Y	N	Do Not Use

VA	Titans Athletics	iOS	N/A	From Now On, LLC	Y	N	Do Not Use
SD	Todd County School District	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
SD	Todd County School District	Android	100-500	Apptegy, Inc.	N	N	High Risk
WY	Uinta County School District	Android	100-500	Blackboard	N	N	Do Not Use
WY	Uinta County School District #	Android	50-100	Your Mobile School APP 2018	--	--	Do Not Use
WA	Vancouver Public Schools	Android	5K-10K	Blackboard	N	N	Do Not Use
WA	Vancouver Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
VA	VBSchools	Android	10K-50K	Intrado Corporation	N	N	Do Not Use
VA	VBSchools	iOS	N/A	Intrado Corporation	N	N	Do Not Use
LA	Vermilion Parish Schools	Android	500-1K	Apptegy, Inc.	N	N	Do Not Use
LA	Vermilion Parish Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AL	Vestavia Hills Athlet-ics	Android	N/A	SIDEARM Sports, a Learfield Company	Y	N	Do Not Use
AL	Vestavia Hills Athlet-ics	iOS	N/A	SIDEARM Sports, a Learfield Company	Y	N	Do Not Use
AL	Vestavia Hills City Schools	Android	500-1K	Blackboard	N	N	Do Not Use
AL	Vestavia Hills City Schools	iOS	N/A	Blackboard	N	N	Do Not Use
AL	VHHS Student Life	Android	100-500	Blackboard	N	N	Do Not Use
AL	VHHS Student Life	iOS	N/A	Blackboard	N	N	Do Not Use
WI	Viroqua Area Schools, WI	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WI	Viroqua Area Schools, WI	Android	500-1K	Apptegy, Inc.	N	N	High Risk
HI	Waiakea Intermedi-ate School	Android	100-500	Educational Net-works, Inc.	N	N	Do Not Use
HI	Waiakea Intermedi-ate School	iOS	N/A	Educational Net-works, Inc.	N	N	High Risk
FL	Wakulla County Schools Focus	Android	100-500	Focus School Soft-ware LLC	--	--	Do Not Use
FL	Wakulla County Schools Focus	iOS	N/A	Focus School Soft-ware LLC	--	--	Do Not Use
KS	Wamego Public Schools	Android	500-1K	Filament Essential Services	N	N	Do Not Use
RI	Warwick Public Schools	Android		Apptegy, Inc.	Y	N	Do Not Use
RI	Warwick Public Schools	iOS	N/A	Apptegy, Inc.	N	N	High Risk
IL	WA Grade School D52	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
IL	WA Grade School D52	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
CT	Watertown Public Schools - CT	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
WV	Wayne Schools, WV	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Wayne Schools, WV	Android	N/A	Apptegy, Inc.	N	N	High Risk

NJ	Wayne Township PS	Android	100-500	Blackboard	N	N	Do Not Use
NJ	Wayne Township PS	iOS	N/A	Blackboard	N	N	Do Not Use
CO	Weld County School District 6	Android	1K-5K	Blackboard	Y	N	Do Not Use
CO	Weld County SD 6	IOS	N/A	Blackboard	Y	Y	Do Not Use
ID	West Ada School District, ID	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
ID	West Ada School District, ID	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
HI	West HI Explorations Acad	Android	10-50	SchoolInfoApp, LLC	N	N	High Risk
HI	West HI Explorations Acad	iOS	N/A	SchoolInfoApp, LLC	N	N	High Risk
VA	Westover Christian Academy	Android	100-500	Apptegy, Inc.	Y	Y	Do Not Use
VA	Westover Christian Academy	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
NE	Westside Community Schools	iOS	N/A	Blackboard	N	N	Do Not Use
AR	Westside Consoli-dated	Android	100-500	Apptegy, Inc.	N	N	High Risk
AR	Westside Consoli-dated	iOS	N/A	Apptegy, Inc.	N	N	High Risk
NE	Westside Warriors	Android	100-500	From Now On, LLC	Y	N	Do Not Use
NE	Westside Warriors	iOS	N/A	From Now On, LLC	Y	N	Do Not Use
KS	Wichita Public Schools	Android	5K-10K	Blackboard	N	N	Do Not Use
KS	Wichita Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
NE	Winnebago Public Schools	Android	10-50	Apptegy, Inc.	N	N	Do Not Use
NE	Winnebago Public Schools, NE	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
ME	Yarmouth School De-partment	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
ME	Yarmouth School De-partment	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
SC	York Preparatory Academy	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
SC	York Preparatory Academy	Android	500-1K	Apptegy, Inc.	N	N	High Risk

11 Appendix C: Community Engagement Platform Apps with Certifications or Promises

iKeepSafe COPPA Safe Harbor Certified CEP Apps							
State	App Name	OS	# Downloads	App Developer	Ads?	Retargeting Ads?	App Score
OH	Buckeye Local JH/HS	Android	1K-5K	SchoolInfoApp, LLC	Y	N	Do Not Use
OH	Buckeye Local School District	iOS	N/A	SchoolInfoApp, LLC	Y	N	Do Not Use
NV	Centennial High School	iOS	N/A	Eldio, LLC	N	N	Do Not Use
NV	Centennial High School	Android	500-1K	Eldio, LLC	N	N	High Risk
NM	Central Consolidated Schools	iOS	N/A	Eldio, LLC	--	--	Unable To Test
NM	Central Consolidated Schools	Android	1K-5K	Eldio, LLC	--	--	Unable To Test
LA	EBR School System	Android	1K-5K	SchoolInfoApp, LLC	Y	N	Do Not Use
LA	EBR School System	iOS	N/A	SchoolInfoApp, LLC	Y	N	Do Not Use
GA	Murray County Schools	Android	1K-5K	SchoolInfoApp, LLC	N	N	Do Not Use
GA	Murray County Schools	iOS	N/A	SchoolInfoApp, LLC	N	N	Do Not Use
LA	Parkway High School	Android	500-1K	SchoolInfoApp, LLC	Y	N	Do Not Use
LA	Parkway High School	iOS	N/A	SchoolInfoApp, LLC	Y	N	Do Not Use
UT	Skyline High School - UT	iOS	N/A	SchoolInfoApp, LLC	N	N	Do Not Use
UT	Skyline High School - UT	Android	500-1K	SchoolInfoApp, LLC	N	N	High Risk
HI	West HI Explorations Acad	Android	10-50	SchoolInfoApp, LLC	N	N	High Risk
HI	West HI Explorations Acad	iOS	N/A	SchoolInfoApp, LLC	N	N	High Risk

1EdTech Certified CEP Apps							
State	App Name	OS	# of Downloads	App Developer	Ads?	Retargeting Ads?	App Score
	Nearpod	iOS	N/A	Nearpod, Inc.	--	--	Do Not Use
	Nearpod	Android	1M-5M	Nearpod, Inc.	--	--	Unable to Test

SDPC CEP Apps							
State	App Name	OS	# of Downloads	App Developer	Ads?	Retargeting Ads?	App Score
	Nearpod	iOS	N/A	Nearpod, Inc.	--	--	Do Not Use
	Nearpod	Android	1M-5M	Nearpod, Inc.	--	--	Unable to Test
	Project Lead The Way	Android	1K-5K	Aventri, Inc.	--	--	Unable to Test

	School Dismissal Manager	Android	10K-50K	School Dismissal Manager	--	--	Unable to Test

Student Privacy Pledge 2020 Signatories - CEP Apps

State	App Name	OS	# of Down-loads	App Developer	Ads?	Retar-geting Ads?	App Score
VA	Alexandria City Public Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
VA	Alexandria City Public Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
VA	Alleghany County Schools	Android	10-50	Intrado Corporation	N	N	Do Not Use
AK	Anchorage School District	Android	10K-50K	Blackboard	N	N	Do Not Use
AK	Anchorage School District	iOS	N/A	Blackboard	N	N	Do Not Use
TX	Anna ISD	iOS	N/A	Blackboard	N	N	Do Not Use
GA	Atlanta Public Schools (APS)	Android	1K-5K	Blackboard	Y	Y	Do Not Use
GA	Atlanta Public Schools (APS)	iOS	N/A	Blackboard	Y	Y	Do Not Use
MD	Baltimore City Public Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
MD	Baltimore City Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
VA	Bedford County School District	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
VA	Bedford County School District	iOS	N/A	Intrado Corporation	N	N	Do Not Use
WV	Berkeley County Schools (WV)	Android	10K-50K	Blackboard	Y	Y	Do Not Use
WV	Berkeley County Schools (WV)	iOS	N/A	Blackboard	Y	Y	Do Not Use
AL	Birmingham City Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
AL	Birmingham City Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
KS	Blue Valley Schools KS	Android	500-1K	Blackboard	N	N	Do Not Use
KS	Blue Valley Schools KS	iOS	N/A	Blackboard	Y	Y	Do Not Use
RI	Bristol Warren Regional SD	Android	100-500	Blackboard	N	N	Do Not Use
RI	Bristol Warren Regional SD	iOS	N/A	Blackboard	N	N	Do Not Use
DE	Caesar Rodney School District	iOS	N/A	Blackboard	N	N	Do Not Use
DE	Caesar Rodney School District	Android	N/A	Blackboard	N	N	Do Not Use
MA	Cambridge Public Schools	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
MA	Cambridge Public Schools	iOS	N/A	Intrado Corporation	N	N	Do Not Use
GA	Carroll County School System	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
IL	CCSD15	Android	1K-5K	Blackboard	N	N	Do Not Use
IL	CCSD15	iOS	N/A	Blackboard	N	N	Do Not Use
PA	Central Dauphin Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
PA	Central Dauphin Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use

SC	Charleston County Schools, SC	Android	1K-5K	Blackboard	N	N	Do Not Use
SC	Charleston County Schools, SC	iOS	N/A	Blackboard	N	N	Do Not Use
DE	Christina School District	Android	1K-5K	Blackboard	N	N	Do Not Use
DE	Christina School District	iOS	N/A	Blackboard	N	N	Do Not Use
TX	Comal ISD	Android	5K-10K	Blackboard	N	N	Do Not Use
TX	Comal ISD	iOS	N/A	Blackboard	N	N	Do Not Use
WI	D.C. Everest School District	Android	500-1K	Blackboard	N	N	Do Not Use
WI	D.C. Everest School District	iOS	N/A	Blackboard	N	N	Do Not Use
MN	Deer River Schools ISD	Android	100-500	Blackboard	N	N	Do Not Use
AZ	Deer Valley Unified SD	Android	1K-5K	Blackboard	N	N	Do Not Use
AZ	Deer Valley Unified SD	iOS	N/A	Blackboard	N	N	Do Not Use
OK	Dickson Public Schools	iOS	N/A	Intrado Corporation	N	N	High Risk
CO	Douglas County SD	Android	1K - 5K	Intrado Corporation	Y	N	Do Not Use
FL	Duval County Public Schools	Android	10K-50K	Blackboard	N	N	Do Not Use
FL	Duval County Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
OH	East Cleveland City Schools	Android	100-500	Blackboard	--	--	Unable To Test
VT	Essex Westford School District	Android	100-500	Blackboard	N	N	Do Not Use
VT	Essex Westford School District	iOS	N/A	Blackboard	N	N	Do Not Use
GA	Floyd Co Schools	Android	10-50	Blackboard	N	N	Do Not Use
GA	Floyd Co Schools	iOS	N/A	Blackboard	N	N	Do Not Use
MI	Gladstone Area Schools	Android	100-500	Intrado Corporation	N	N	Do Not Use
ND	Grand Forks 1 School District	iOS	N/A	Blackboard	N	N	Do Not Use
ND	Grand Forks Public Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
NE	Grand Island Public Schools	Android	100-500	Intrado Corporation	N	N	Do Not Use
SC	Greenville County Schools	Android	5K-10K	Intrado Corporation	Y	N	Do Not Use
NY	Hamburg CSD	Android	100-500	Intrado Corporation	N	N	Do Not Use
NY	Hamburg CSD	iOS	N/A	Intrado Corporation	N	N	Do Not Use
TN	Hamilton County Schools	Android	1K-5K	Intrado Corporation	--	--	Do Not Use
AL	Hartselle City Schools	Android	500-1K	Blackboard	N	N	Do Not Use
AL	Hartselle City Schools	iOS	N/A	Blackboard	N	N	Do Not Use
TX	Hays CISD	Android	5K-10K	Blackboard	Y	Y	Do Not Use
TX	Hays CISD	iOS	N/A	Blackboard	Y	Y	Do Not Use
MD	HCPSS	Android	10K-50K	Intrado Corporation	N	N	Do Not Use
MD	HCPSS	iOS	N/A	Intrado Corporation	N	N	Do Not Use
GA	Henry County Schools (GA)	Android	500-1K	Blackboard	Y	Y	Do Not Use
OH	Hudson City Schools - OH	Android	1K-5K	Blackboard	Y	Y	Do Not Use
OH	Hudson City Schools - OH	iOS	N/A	Blackboard	Y	Y	Do Not Use
NY	Hudson Falls CSD	Android	N/A	Intrado Corporation	N	N	Do Not Use

NY	Hudson Falls CSD	iOS	500-1k	Intrado Corporation	N	N	Do Not Use
TX	Iola Independent School Distri	Android	100-500	Blackboard	N	N	Do Not Use
MS	Jackson Public Schools - MS	Android	1K-5K	Blackboard	N	N	Do Not Use
MS	Jackson Public Schools - MS	iOS	N/A	Blackboard	N	N	Do Not Use
ND	Jamestown 1-ND	Android	1K-5K	Blackboard	Y	Y	Do Not Use
ND	Jamestown 1-ND	iOS	N/A	Blackboard	Y	N	Do Not Use
KY	JCPS	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
KY	JCPS	iOS	N/A	Intrado Corporation	N	N	Do Not Use
AL	Jefferson County SD	Android	100-500	Blackboard	N	N	Do Not Use
AL	Jefferson County SD	iOS	N/A	Blackboard	N	N	Do Not Use
IA	Johnston Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
IA	Johnston Schools	iOS	N/A	Blackboard	N	N	Do Not Use
AK	Kenai Peninsula Borough SD	Android	1K-5K	Blackboard	N	N	Do Not Use
AK	Kenai Peninsula Borough SD	iOS	N/A	Blackboard	N	N	Do Not Use
TX	La Feria ISD	Android	500-1K	Intrado Corporation	Y	N	Do Not Use
KS	Leavenworth USD 453	Android		Blackboard	Y	N	Do Not Use
KS	Leavenworth USD 453	iOS	N/A	Blackboard	Y	N	Do Not Use
CO	Lewis-Palmer SD #38	Android	500-1K	Blackboard	Y	N	Do Not Use
CO	Lewis-Palmer SD #38	IOS	N/A	Blackboard	Y	N	Do Not Use
RI	Lincoln Public Schools	Android	5-10	Blackboard	N	N	Do Not Use
RI	Lincoln Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
AR	Little Rock School District	Android	1K-5K	Blackboard	Y	N	Do Not Use
AR	Little Rock School District	iOS	N/A	Blackboard	Y	N	Do Not Use
MS	Madison County Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
MS	Madison County Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
AK	Matanuska-Susitna Borough SD	Android	1K-5K	Blackboard	N	N	Do Not Use
AK	Matanuska-Susitna Borough SD	iOS	N/A	Blackboard	N	N	Do Not Use
ND	McKenzie County School Dist.	Android	500-1K	Blackboard	N	N	Do Not Use
ND	McKenzie County School Dist.	iOS	N/A	Blackboard	N	N	Do Not Use
NH	Merrimack School District	Android	500-1k	Intrado Corporation	N	N	Do Not Use
NH	Merrimack SD	iOS	N/A	Intrado Corporation	N	N	Do Not Use
TN	Metro Nashville Public Schools	Android	100-500	Intrado Corporation	N	N	Do Not Use
TN	Metro Nashville Public Schools	iOS	N/A	Intrado Corporation	N	N	Do Not Use
TX	Midland ISD	Android	1K-5K	Blackboard	N	N	Do Not Use
TX	Midland ISD	iOS	N/A	Blackboard	N	N	Do Not Use
MD	Montgomery Public Schools	Android	10K-50K	Blackboard	Y	Y	Do Not Use

MI	Mount Clemens Community School	Android	50-100	Appazur Solutions Inc.	N	N	Do Not Use
MI	Mount Clemens Community School	iOS	N/A	Appazur Solutions Inc.	N	N	Do Not Use
MN	MySPPS Saint Paul Public Schoo	Android	5K-10K	Blackboard	N	N	Do Not Use
MN	MySPPS St Paul Schools	iOS	N/A	Blackboard	N	N	Do Not Use
	Nearpod	iOS	N/A	Nearpod, Inc.	--	--	Do Not Use
	Nearpod	Android	1M-5M	Nearpod, Inc.	--	--	Unable to Test
CT	New Haven Public Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
CT	Newtown Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
ND	Oakes Public Schools	Android	500-1K	Blackboard	Y	Y	Do Not Use
ND	Oakes Public Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
FL	OCPS	Android	10K-50K	Intrado Corporation	Y	Y	Do Not Use
FL	OCPS	iOS	N/A	Intrado Corporation	Y	Y	Do Not Use
KS	Olathe Public Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
KS	Olathe Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
NC	Onslow County Schools	Android	1K-5K	Blackboard	N	N	Do Not Use
FL	Palm Beach County School Dist	Android	10K-50K	Intrado Corporation	Y	Y	Do Not Use
FL	Palm Beach County School Dist	iOS	N/A	Intrado Corporation	Y	Y	Do Not Use
AL	Pell City Schools	Android	100-500	Blackboard	N	N	Do Not Use
AL	Pell City Schools	iOS	N/A	Blackboard	N	N	Do Not Use
PA	Phoenixville Area SD	Android	100-500	Intrado Corporation	Y	N	Do Not Use
MO	Portageville School District	iOS	N/A	Intrado Corporation	N	N	Do Not Use
MD	Prince George's County PS	Android	10K-50K	Blackboard	Y	Y	Do Not Use
MD	Prince George's County PS	iOS	N/A	Blackboard	Y	Y	Do Not Use
RI	Providence Schools	Android	100-500	Blackboard	Y	Y	Do Not Use
DE	Red Clay CSD	Android	500-1K	Blackboard	N	N	Do Not Use
KY	Red Oak ISD	Android	1K-5K	Blackboard	N	N	Do Not Use
KY	Red Oak ISD	iOS	N/A	Blackboard	N	N	Do Not Use
SC	Richland One	Android	1K-5K	Blackboard	N	N	Do Not Use
SC	Richland One	iOS	N/A	Blackboard	N	N	Do Not Use
MO	Ritenour Schools	Android	1K-5K	Blackboard	Y	Y	Do Not Use
MO	Ritenour Schools	iOS	N/A	Blackboard	Y	Y	Do Not Use
AR	Rogers Public Schools - AR	Android	1K-5K	Blackboard	Y	N	Do Not Use
AR	Rogers Public Schools - AR	iOS	N/A	Blackboard	N	N	Do Not Use
NM	Roswell Independent Schools	Android	1K-5K	Intrado Corporation	N	N	Do Not Use
NM	Roswell Independent Schools	iOS	N/A	Intrado Corporation	N	N	Do Not Use
ND	Rugby Public Schools	Android	100-500	Blackboard	N	N	Do Not Use
ND	Rugby Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
WA	San Juan Island SD	Android	100-500	Blackboard	N	N	Do Not Use
WA	San Juan Island SD	iOS	N/A	Blackboard	N	N	Do Not Use

IN	Scott County School District 2	Android	100-500	Intrado Corporation	N	N	Do Not Use
VA	Scott County VA Schools	Android	10-50	Intrado Corporation	N	N	Do Not Use
TN	Sevier County School System	Android	1K-5K	Blackboard	N	N	Do Not Use
TN	Sevier County School System	iOS	N/A	Blackboard	N	N	Do Not Use
DE	Smyrna School District	Android	500-1K	Intrado Corporation	N	N	Do Not Use
WY	Uinta County School District	Android	100-500	Blackboard	N	N	Do Not Use
WA	Vancouver Public Schools	Android	5K-10K	Blackboard	N	N	Do Not Use
WA	Vancouver Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use
VA	VBSchools	Android	10K-50K	Intrado Corporation	N	N	Do Not Use
VA	VBSchools	iOS	N/A	Intrado Corporation	N	N	Do Not Use
AL	Vestavia Hills City Schools	Android	500-1K	Blackboard	N	N	Do Not Use
AL	Vestavia Hills City Schools	iOS	N/A	Blackboard	N	N	Do Not Use
AL	VHHS Student Life	Android	100-500	Blackboard	N	N	Do Not Use
AL	VHHS Student Life	iOS	N/A	Blackboard	N	N	Do Not Use
NJ	Wayne Township PS	Android	100-500	Blackboard	N	N	Do Not Use
NJ	Wayne Township PS	iOS	N/A	Blackboard	N	N	Do Not Use
CO	Weld County School District 6	Android	1K-5K	Blackboard	Y	N	Do Not Use
CO	Weld County SD 6	IOS	N/A	Blackboard	Y	Y	Do Not Use
NE	Westside Community Schools	iOS	N/A	Blackboard	N	N	Do Not Use
KS	Wichita Public Schools	Android	5K-10K	Blackboard	N	N	Do Not Use
KS	Wichita Public Schools	iOS	N/A	Blackboard	N	N	Do Not Use

Vendor-Asserted COPPA Compliance CEP Apps

State	App Name	OS	# of Down-loads	App Developer	Ads?	Retar-geting Ads?	App Score
NC	Alamance-Burlington Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
NC	Alamance-Burlington Schools	Android		Apptegy, Inc.	N	N	High Risk
MT	Anaconda School District	Android	50-100	Apptegy, Inc.	N	N	High Risk
TX	Anna Coyote Athletics	Android	100-500	Mascot Media, LLC	Y	N	Do Not Use
TX	Anna Coyote Athletics	iOS	N/A	Mascot Media, LLC	Y	N	Do Not Use
SD	Bennett County School District	Android	100-500	Apptegy, Inc.	Y*	N	Do Not Use
SD	Bennett County School District	iOS	N/A	Apptegy, Inc.	Y*	N	Do Not Use
ME	Biddeford School District, ME	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
ME	Biddeford School District, ME	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
KY	Boone County Schools	Android	1K-5K	SchoolPointe, Inc.	N	N	Do Not Use
KY	Boone County Schools	iOS	N/A	SchoolPointe, Inc.	N	N	Do Not Use

GA	Bryan County Schools, GA	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
GA	Bryan County Schools, GA	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
NC	Buncombe County Schools, NC	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
NC	Buncombe County Schools, NC	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
KS	Burlington Schools	Android	1K-5K	Gabbart Communi-cations	N	N	Do Not Use
KS	Burlington Schools	iOS	N/A	Gabbart Communi-cations	N	N	Do Not Use
IA	Camanche Community School	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
IA	Camanche Community School	Android	100-500	Apptegy, Inc.	N	N	High Risk
LA	CCSS Wildcats	Android	N/A	Apptegy, Inc.	N	N	High Risk
LA	CCSS Wildcats	iOS	N/A	Apptegy, Inc.	N	N	High Risk
SD	Chamberlain School District	Android	100-500	Apptegy, Inc.	Y	N	Do Not Use
SD	Chamberlain School District	iOS	N/A	Apptegy, Inc.	Y	N	Do Not Use
WY	Cody Public Schools - Park 6	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WY	Cody Public Schools - Park 6	Android	500-1K	Apptegy, Inc.	N	N	High Risk
OK	Collinsville Public Schools	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
OK	Collinsville Public Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
MT	Corvallis MT School Dist	Android	100-500	Apptegy, Inc.	N	N	High Risk
MT	Corvallis MT School Dist	iOS	N/A	Apptegy, Inc.	N	N	High Risk
NJ	Cresskill Public Schools	Android	50-100	Apptegy, Inc.	N	N	Do Not Use
NJ	Cresskill Public Schools	iOS	N/A	Apptegy, Inc.	N	N	High Risk
NE	DC West Community Schools	Android	100-500	Filament Essential Services	Y	N	Do Not Use
NE	DC West Community Schools	iOS	N/A	Filament Essential Services	Y	N	Do Not Use
KS	Dodge City Public Schools	Android	500-1K	Gabbart Communi-cations	N	N	Do Not Use
KS	Dodge City Public Schools	iOS	N/A	Gabbart Communi-cations	N	N	Do Not Use
CO	Dolores School District	Android	100	Bluetree Apps	N	N	Do Not Use
CO	Dolores School District	iOS	N/A	Bluetree Apps	N	N	Do Not Use
IN	East Allen County Schools	Android	1K-5K	Apptegy, Inc.	Y	N	Do Not Use
IN	East Allen County Schools	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
IN	East Noble	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
IN	East Noble	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
OH	Edgewood City Schools, OH	Android	1K-5K	Apptegy, Inc.	Y	N	Do Not Use
ME	Ellsworth School Department	Android	10-50	Apptegy, Inc.	N	N	Do Not Use
ME	Ellsworth School Department	iOS	N/A	Apptegy, Inc.	N	N	High Risk
IL	Essexville-Hampton Schools	Android	50-100	Apptegy, Inc.	N	N	Do Not Use

AR	eStem Public Charter Schools	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
AR	eStem Public Charter Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AR	Forrest City Mustangs	Android	100-500	Gabbart Communi-cations	N	N	Do Not Use
AR	Fort Smith PS Athletics	Android	50-100	Mascot Media, LLC	Y	N	Do Not Use
AR	Fort Smith PS Athletics	iOS	N/A	Mascot Media, LLC	Y	Y	Do Not Use
KY	Garrard County Schools, KY	Android	N/A	Apptegy, Inc.	N	N	Do Not Use
KY	Garrard County Schools, KY	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AZ	GUSD1	Android	100-500	Apptegy, Inc.	N	N	High Risk
AZ	GUSD1	iOS	N/A	Apptegy, Inc.	N	N	High Risk
AL	Haleyville City Schools	Android	50-100	Apptegy, Inc.	N	N	Do Not Use
AL	Haleyville City Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Hancock County Schools, WV	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
WV	Hancock County Schools, WV	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Harrison County Schools, WV	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
WV	Harrison County Schools, WV	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
KS	Hays USD 489, KS	Android	100-500	Apptegy, Inc.	Y	Y	Do Not Use
KS	Hays USD 489, KS	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
KS	Hesston Swathers	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
KS	Hesston Swathers	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
NV	Humboldt County Schools, NV	Android	100-500	Apptegy, Inc.	N	N	High Risk
AR	Jacksonville North Pulaski, AR	Android	500-1K	Apptegy, Inc.	Y	N	Do Not Use
AR	Jacksonville North Pulaski, AR	iOS	N/A	Apptegy, Inc.	Y	N	Do Not Use
AR	Jacksonville Titans Athletics	Android	50-100	Mascot Media, LLC	Y	N	Do Not Use
AR	Jacksonville Titans Athletics	iOS	N/A	Mascot Media, LLC	Y	N	Do Not Use
KS	Jefferson West USD 340	Android	100-500	Apptegy, Inc.	Y	Y	Do Not Use
KS	Jefferson West USD 340	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
KY	Johnson County Schools	Android	500-1K	Apptegy, Inc.	N	N	Do Not Use
KY	Johnson County Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
KY	Kenton County School District	iOS	N/A	SchoolPointe, Inc.	N	N	Do Not Use
KY	Kenton County School District	Android	1K-5K	SchoolPointe, Inc.	N	N	High Risk
WI	Kewaskum School District	Android	100-500	SchoolPointe, Inc.	N	N	Do Not Use
WI	Kewaskum School District	iOS	N/A	SchoolPointe, Inc.	--	--	Do Not Use
WY	LCSD 1	iOS	N/A	Gabbart Communi-cations	N	N	Do Not Use
WY	Lincoln County School District	Android	50-100	Gabbart Communi-cations	N	N	Do Not Use
MT	Malta Public Schools	Android	50-100	Apptegy, Inc.	N	N	Do Not Use

MT	Malta Public Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
TX	Mansfield ISD Athletics	Android	100-500	Mascot Media, LLC	Y	N	Do Not Use
TX	Mansfield ISD Athletics	iOS	N/A	Mascot Media, LLC	Y	N	Do Not Use
VT	Maple Run Unified School, VT	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
VT	Maple Run Unified School, VT	iOS	N/A	Apptegy, Inc.	N	N	Some Risk
ME	Maranacook Area Schools	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
ME	Maranacook Area Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Marion County Schools, WV	Android	500-1K	Apptegy, Inc.	N	N	Do Not Use
WV	Marion County Schools, WV	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
KY	Marshall County Schools	Android	1K-5K	SchoolPointe, Inc.	--	--	Unable To Test
KY	Marshall County Schools	iOS	N/A	SchoolPointe, Inc.	--	--	Unable To Test
MO	Marshall Public Schools, MO	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
MO	Marshall Public Schools, MO	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
AR	Mayflower School District, AR	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
AR	Mayflower School District, AR	iOS	N/A	Apptegy, Inc.	N	N	High Risk
	Minga	Android	10K-50K	Minga	--	--	Unable to Test
	Minga	iOS	N/A	Minga	--	--	Unable to Test
MO	Monroe City R1 School District	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
MO	Monroe City R1 School District	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Morgan County Schools, WV	Android	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Morgan County Schools, WV	iOS	100-500	Apptegy, Inc.	N	N	Do Not Use
ME	MSAD #1	Android	N/A	Apptegy, Inc.	N	N	Do Not Use
ME	MSAD #1	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
FL	MySDMC Focus	Android	5K-10K	Focus School Soft-ware LLC	N	N	Do Not Use
FL	MySDMC Focus	iOS	N/A	Focus School Soft-ware LLC	N	N	Do Not Use
	Nearpod	iOS	N/A	Nearpod, Inc.	--	--	Do Not Use
	Nearpod	Android	1M-5M	Nearpod, Inc.	--	--	Unable to Test
CT	New Fairfield Public Schools	Android	50-100	Apptegy, Inc.	N	N	High Risk
WV	OH County Schools, WV	Android	100-500	Apptegy, Inc.	Y	Y	Do Not Use
WV	OH County Schools, WV	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
OK	Oologah-Talala Public Schools	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
OK	Oologah-Talala Public Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
LA	Ouachita Parish Schools	Android	500-1K	Gabbart Communi-cations	N	N	Do Not Use

LA	Ouachita Parish Schools	iOS	N/A	Gabbart Communications	N	N	Do Not Use
FL	Palm Beach County SIS Gateway	Android	5K-10K	Focus School Software LLC	Y	N	Do Not Use
FL	Palm Beach County SIS Gateway	iOS	N/A	Focus School Software LLC	N	N	Do Not Use
WV	PCS Connect	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
WV	PCS Connect	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
IL	Pikeland CUSD #10, IL	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
IL	Pikeland CUSD #10, IL	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AR	Pulaski County SSD, AR	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
AR	Pulaski County SSD, AR	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
CA	Rincon Valley USD, CA	Android	500-1K	Apptegy, Inc.	N	N	High Risk
NM	Rio Rancho Public Schools, NM	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
NM	RioRancho Public Schools, NM	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
AR	RPS Athletics	iOS	N/A	Mascot Media, LLC	Y	N	Do Not Use
CO	Sanford School District	IOS	N/a	Apptegy, Inc.	N	N	Do Not Use
CO	Sanford School District, CO	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
NH	SAU 54 Rochester, NH	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
NH	SAU 54 Rochester, NH	iOS	N/A	Apptegy, Inc.	N	N	High Risk
	School Dismissal Manager	Android	10K-50K	School Dismissal Manager	--	--	Unable to Test
	School Dismissal Manager (SDM)	iOS	N/A	School Dismissal Manager	--	--	Unable to Test
WI	School District of Bloomer	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
WI	School District of Bloomer	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
SD	Sioux Falls Schools	Android	500-1K	Apptegy, Inc.	N	N	Do Not Use
SD	Sioux Falls Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Summers County Schools	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
WV	Summers County Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
OK	Tecumseh Public Schools	Android	1K-5K	Apptegy, Inc.	N	N	Do Not Use
OK	Tecumseh Public Schools, OK	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
ID	The Village Charter School	Android	50-100	Apptegy, Inc.	N	N	Do Not Use
ID	The Village Charter School	iOS	N/A	Apptegy, Inc.	N	N	High Risk
OK	Thomas Fay Custer Schools	Android	N/A	Gabbart Communications	N	N	Do Not Use
OK	Thomas Fay Custer Schools	iOS	N/A	Gabbart Communications	N	N	Do Not Use
NJ	Tinton Falls School District	Android	N/A	Apptegy, Inc.	N	N	Do Not Use
NJ	Tinton Falls School District	iOS	N/A	Apptegy, Inc.	N	N	High Risk
SD	Todd County School District	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
SD	Todd County School District	Android	100-500	Apptegy, Inc.	N	N	High Risk
LA	Vermilion Parish Schools	Android	500-1K	Apptegy, Inc.	N	N	Do Not Use
LA	Vermilion Parish Schools	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use

AL	Vestavia Hills Athletics	Android	N/A	SIDEARM Sports, a Learfield Company	Y	N	Do Not Use
AL	Vestavia Hills Athletics	iOS	N/A	SIDEARM Sports, a Learfield Company	Y	N	Do Not Use
WI	Viroqua Area Schools, WI	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WI	Viroqua Area Schools, WI	Android	500-1K	Apptegy, Inc.	N	N	High Risk
FL	Wakulla County Schools Focus	Android	100-500	Focus School Software LLC	--	--	Do Not Use
FL	Wakulla County Schools Focus	iOS	N/A	Focus School Software LLC	--	--	Do Not Use
KS	Wamego Public Schools	Android	500-1K	Filament Essential Services	N	N	Do Not Use
RI	Warwick Public Schools	Android		Apptegy, Inc.	Y	N	Do Not Use
RI	Warwick Public Schools	iOS	N/A	Apptegy, Inc.	N	N	High Risk
IL	WA Grade School D52	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
IL	WA Grade School D52	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
CT	Watertown Public Schools - CT	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
WV	Wayne Schools, WV	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
WV	Wayne Schools, WV	Android	N/A	Apptegy, Inc.	N	N	High Risk
ID	West Ada School District, ID	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
ID	West Ada School District, ID	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
VA	Westover Christian Academy	Android	100-500	Apptegy, Inc.	Y	Y	Do Not Use
VA	Westover Christian Academy	iOS	N/A	Apptegy, Inc.	Y	Y	Do Not Use
AR	Westside Consolidated	Android	100-500	Apptegy, Inc.	N	N	High Risk
AR	Westside Consolidated	iOS	N/A	Apptegy, Inc.	N	N	High Risk
NE	Winnebago Public Schools	Android	10-50	Apptegy, Inc.	N	N	Do Not Use
NE	Winnebago Public Schools, NE	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
ME	Yarmouth School Department	Android	100-500	Apptegy, Inc.	N	N	Do Not Use
ME	Yarmouth School Department	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
SC	York Preparatory Academy	iOS	N/A	Apptegy, Inc.	N	N	Do Not Use
SC	York Preparatory Academy	Android	500-1K	Apptegy, Inc.	N	N	High Risk