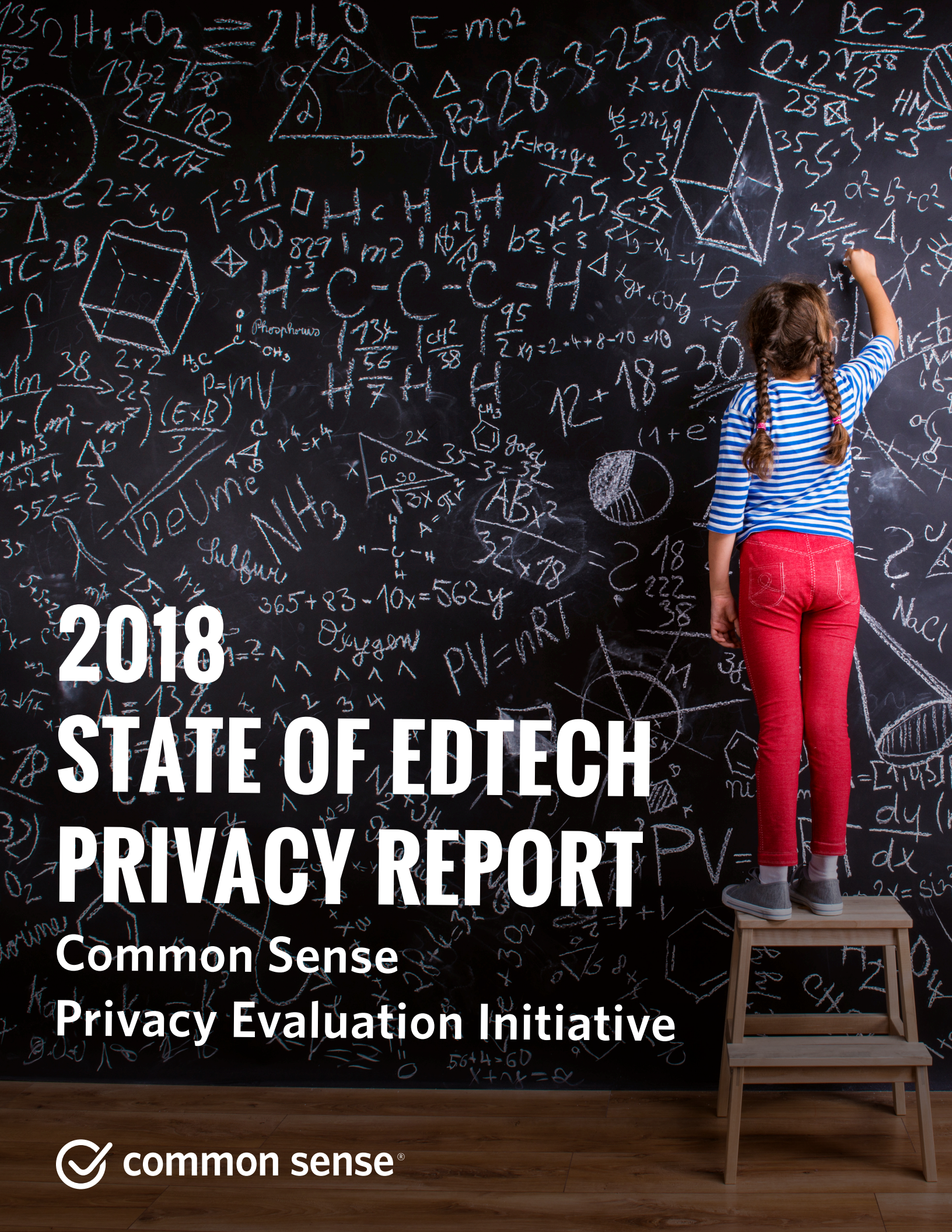


2018 STATE OF EDTECH PRIVACY REPORT

Common Sense Privacy Evaluation Initiative

common sense®

CREDITS

Authors: Girard Kelly
Jeff Graham
Bill Fitzgerald

Suggested citation: Kelly, G., Graham, J., & Fitzgerald, B. (2018). 2018 State of Edtech Privacy Report, Common Sense Privacy Evaluation Initiative. San Francisco, CA: Common Sense.

2018 STATE OF EDTECH PRIVACY REPORT

Common Sense Privacy Evaluation Initiative

Common Sense is grateful for the generous support and underwriting that funded this research report from the Michael & Susan Dell Foundation and the Bill & Melinda Gates Foundation.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

While mainstream media fixates on privacy shortcomings of big tech and social media companies, far less attention is paid to the privacy and security practices of technology platforms that impact tens of millions of children on a daily basis: educational software. About 94 percent of U.S. schools have classrooms that are "connected," allowing students to access applications that help them practice skills and expand their knowledge — while also collecting and potentially using their personal data for unintended purposes.

In 2014, leaders of several large school districts approached Common Sense Education to help them address this critical disparity. The result was a partnership with more than 150 school districts across the country with the common goal of making the privacy practices of education technology products more transparent and accessible for parents, teachers, and students by creating a comprehensive approach to privacy evaluations.

This report represents the culmination of a three-year examination into how student information is collected, used, and disclosed. It evaluates 100 of the most popular applications and services used in educational technology using two broad criteria: transparency and quality.

Our overall findings indicate a widespread lack of transparency and inconsistent privacy and security practices. Nearly all the educational technology applications and services evaluated either do not clearly define safeguards taken to protect child or student information, or lack a detailed privacy policy. Only 10 percent of the applications or services met our minimum criteria for transparency and quality in their policies. Our findings are not a sign that a vendor is doing anything unethical but could mean, based on how the application or service is used, that it may be violating federal or state laws. Our privacy-evaluation process uses only publicly available policies and is not an observational evaluation or assessment of a company's actual practices.

In evaluating 25 indicators for safety, privacy, security, and compliance, our research uncovered key findings in several important areas:

- **Third-party marketing**: Thirty-eight percent of educational technologies evaluated indicate they may use children's personal and nonpersonal information for third-party marketing.
- **Advertising**: Forty percent indicate they may display contextual ads based on webpage content, and 29 percent indicate they may display behavioral ads based on information collected from use of the service.

- **Tracking**: Among web-based services, 37 percent indicate collected information can be used by tracking technologies and third-party advertisers, 21 percent indicate collected data may be used to track visitors after they leave the site, and 30 percent indicate they ignore "do not track" requests or other mechanisms to opt out.
- **Profiling**: Ten percent indicate they may create and target profiles of their users.
- **Data transfer**: Seventy-four percent indicate they maintain the right to transfer any personal information collected to a third party if the company is acquired, merges, or files for bankruptcy.
- **Moderation of interactions and content**: Only 11 percent indicate they moderate social interactions between users, if this service is available. Additionally, only 14 percent indicate they review user-generated content to remove non-age-appropriate content, such as references to gambling, alcohol, violence, or sex.
- **Visible personal information**: Fifty percent indicate they may allow children's information to be made publicly visible.

To be sure, there are areas where vendors also scored well. We found, for example, that 92 percent indicate they use reasonable security standards to protect their users' information. In addition, 65 percent affirm that they do not sell, rent, lease, or trade users' personally identifiable information. That said, 33 percent were non-transparent on this critical issue.

The overall lack of transparency, which was pervasive across nearly all indicators we examined, is especially troubling. In our analysis, transparency was a reliable indicator of quality; applications and services that were more transparent also tended to engage in qualitatively better privacy and security practices. When these practices are not transparently disclosed, there can be no future expectation or trust on behalf of parents, teachers, schools, or districts about how collected information from children and students will be handled to meet their expectations of privacy.

We fully recognize that a number of factors conspire to make the landscape a particularly thorny one, marred by complex laws and statutes, technical issues and legacies, and a lack of clarity among educators and parents.

Nevertheless, educational technology platforms serve an especially vulnerable population. It is vital that educators, parents, and policymakers engage in an open dialogue with vendors to build solutions that strengthen our children's privacy and security protections. This report starts that critical conversation, one that will continue with a follow-up report in 2019, covering an even larger group of applications and services.

INTRODUCTION

The Common Sense Privacy Evaluation Initiative provides a framework by which to analyze and describe information in privacy policies so parents and teachers can make smart and informed choices about the learning tools they use with their children and students, while schools and districts can participate in evaluating the technology used in K–12 classrooms. Today, with the involvement of over 140 schools and districts, we are working in collaboration with software developers to bring greater transparency to privacy policies across the industry. We have been collecting and incorporating feedback from stakeholders about how to share the results of our privacy evaluations since July 2015. Since that time, we have spoken with numerous teachers, students, parents, developers, vendors, privacy advocates, and industry representatives about their perspectives on privacy.

This 2018 State of Edtech Privacy Report represents the culmination of our research over the past three years in evaluating hundreds of education technology-related applications and services. The report limits its findings to 100 privacy policies from popular edtech applications and services, as determined from interviews with various teachers, schools, and districts as well as total App Store downloads during the past 12 months. These applications and services provide a representative sample of the wide range of educational technologies that include educational games and tools for communication, collaboration, formative assessment, student feedback, content creation, and delivery of instructional content. These types of applications and services are currently used by millions of children at home and by tens of millions of students in classrooms across the country. To effectively evaluate the policies of all these applications and services, a comprehensive assessment framework was developed based on existing federal and state law, as well as privacy and security universal principles. This framework incorporates over 150 privacy- and security-related questions that are commonly expected to be disclosed in a vendor's policies in an educational context. In addition, both qualitative and quantitative methods were developed to determine both the particular issues vendors actually disclose in their policies and the meanings behind those disclosures.

Of the applications and services we evaluated for this report, each had a privacy policy and/or terms of service available on its website at the time of our evaluation, and in all cases where a mobile application also was made available, that product provided a link

to the same privacy policy on its website from the appropriate App Store. However, this report limits its analysis to the policies of applications and services that are publicly available prior to use, as described in our Evaluation Process section. Our findings may not reflect actual usage by applications and services, given that additional student data privacy agreements may exist privately between the vendor and schools or districts. These additional agreements not made available for our evaluation process may define, among many things, how student information can be collected, used, and disclosed. In addition, many popular edtech applications or services that are not reflected in this report are available without sufficient policies. In many instances, popular edtech applications or services do not provide privacy policies prior to use, provide broken links to missing policies, or do not contain policies at all. App stores could play a leading role in improving the privacy practices of vendors by verifying that all services contain links to valid privacy policies.

Our overall findings indicate a widespread lack of transparency and inconsistent privacy and security practices. Our key findings are illustrative of current trends in the edtech industry. The key findings focus on these general areas: encryption, effective policy dates, selling data, third-party marketing, traditional advertising, behavioral advertising, third-party tracking, and the onward transfer of data to third parties.

Our key findings are that:

1. A majority of applications and services use default encryption of information for login and account creation.

2. A majority of applications and services disclose an effective date or version number of their policies.

3. A majority of applications and services disclose that they do not rent, lease, trade, or sell data, but many are non-transparent.

4. A majority of applications and services are non-transparent or explicitly allow third-party marketing.

5. A majority of applications and services are non-transparent or explicitly allow traditional advertising.

6. A roughly equivalent percentage of applications and services have either non-transparent, better, or worse practices about behavioral advertising.

7. A majority of applications and services are non-transparent or explicitly allow third-party tracking.

8. A majority of applications and services are non-transparent or explicitly track users across other websites.

9. A majority of applications and services are non-transparent about creating ad profiles.

10. A majority of applications and services are non-transparent or explicitly allow the onward transfer of data.

This report would have not been possible without support from the Privacy Evaluation Initiative Consortium, which includes over 140 schools and districts that help inform our work and use our privacy evaluations as part of their vetting process for educational applications and services used in the classroom.[1] The findings in this report were prepared by the Privacy Evaluation Initiative team members, which include Bill Fitzgerald, Jeff Graham, and Girard Kelly, who are leaders and experts in the fields of privacy and security with diverse backgrounds in education, entrepreneurship, computer science, ethics, law, and public policy. We believe that advocacy, parental choice, and school-based decision making will be more effective if users are provided with comprehensive and up-to-date information on the state of privacy for edtech applications and services. We hope this data will help show the impact that privacy and security practices have on the lives of millions of children and students who use educational technology every day and help support meaningful and positive changes in those practices. The following report illustrates our methodologies, results, categorical concerns, and key findings regarding privacy and security practices used by 100 popular edtech applications and services.

1 Common Sense Media, *School Districts Inform Our Work*, https://www.commonsense.org/education/privacy/about/districts; Common Sense Media, *The Privacy Evaluation Initiative Consortium*, https://www.commonsense.org/education/privacy/about/participants.

METHODOLOGY

Our evaluation process for edtech applications and services attempts to address some of the common barriers to effectively evaluating privacy practices. Privacy concerns and needs vary widely based on the type of application or service and the context in which it is used. For example, it makes sense for a student-assessment system to collect a home address or other personal information. However, it would not make sense for an online calculator to collect a student's home address or other types of personal information. Therefore, our evaluation process pairs a transparency evaluation with a qualitative evaluation. This provides the ability to track the information a policy discloses as well as the strengths and weaknesses of how a policy discloses that information. Lastly, our evaluation process includes reviewer-written summary evaluations that highlight the implications of the application or service's privacy practices alongside the goals and contexts within which the service may be used. More information about our privacy evaluations and summaries are available at https://www.commonsense.org/education/privacy.

Evaluation Process

The privacy evaluation process contains four steps:

1. Overview: Select a product to evaluate the details of the various policies of the application or service.
2. Triage: Answer initial observational questions not related to the policy text itself but rather related to the vendor's privacy and security practices.
3. Evaluation: Answer questions about whether or not the text of the policy discloses particular issues. Questions are composed of the following details:
    a. Transparency selection: Do the policies discuss the issue(s) raised in the question?
    b. Qualitative selection: Do the policies indicate whether or not the vendor engages in the particular practice described?
    c. Notes: Is there anything noteworthy, exceptional, or egregious regarding the details of the question?
    d. Policy references: Can text within the policies be highlighted and associated with the particular question selected?

4. Summary: Create a summary of the application or service and describe the various policy details for each of the concerns related to safety, privacy, security, and compliance.[2,3]

In addition to this evaluation process, our team also published an information security primer.[4] While we do not run all the additional security-related tests as part of every evaluation, the primer is a useful resource, and we have used it to support multiple products addressing security issues.

Question Framework

The privacy evaluation process combines transparency and qualitative questions in a single streamlined framework. This requires organizing all the questions into categories and sections derived from the Fair Information Practice Principles (FIPPs)[5] that underlie international privacy laws and regulations. In addition, the questions and the categories that organize them all are mapped to a range of statutory, regulatory, and technical resources that provide background information on why each question is relevant to the privacy evaluation process.[6] For example, the following evaluation question requires a reviewer to read the policies of the application or service and determine whether or not it transparently discloses the issue raised in the question by providing a yes or no response:

> *Question: Do the policies clearly indicate whether or not the vendor collects personally identifiable information (PII)?*

If the reviewer responds yes to this question, that means the application or service discloses whether or not it collects personally identifiable information, and the overall transparency score is increased. Given a yes transparent response to this question, the reviewer is then asked a follow-up question of whether or not the application or service discloses it engages in the particular practice described. A yes or no response that personally identifiable information is or is not collected will increase or decrease the

---

2 Common Sense Media, *Evaluating Apps, Step by Step* (2016), https://www.commonsense.org/education/privacy/blog/evaluating-apps-step-by-step.

3 Common Sense Media, *Needles, Haystacks, and Policies* (2017), https://www.commonsense.org/education/privacy/blog/needles-haystacks-policies.

4 Common Sense Media, *Information Security Primer for Evaluating Educational Software* (2016), https://www.commonsense.org/education/privacy/security-primer.

5 Common Sense Media, *Privacy Evaluation Questions – Fair Information Practice Principles*, https://www.commonsense.org/education/privacy/questions/categories.

6 Common Sense Media, *Navigate by Category*, https://www.commonsense.org/education/privacy/questions/navigate-by-category.

overall quality score based on whether the practices described are considered qualitatively better or worse for the purposes of our evaluation process. The following discussion of evaluation scores describes in more detail how responses to questions affect the overall roll-up score for an application or service.

Evaluation Tiers

In schools and districts, people make decisions about privacy based on their specific needs — and these needs can vary between districts and schools. The privacy evaluation process is designed to support and augment local expertise, not replace it. The evaluation process incorporates these specific needs and the decision-making processes of schools and districts into the following three tiers[7]:

1. *Use Responsibly*, which indicates that the application or service meets our minimum criteria but more research should be completed prior to use;
2. *Use with Caution*, which indicates that the application or service does not clearly define the safeguards to protect child or student information; and
3. *Not Recommended*, which indicates that the application or service does not support encryption or lacks a detailed privacy policy.

PRIVACY EVALUATION TIERS

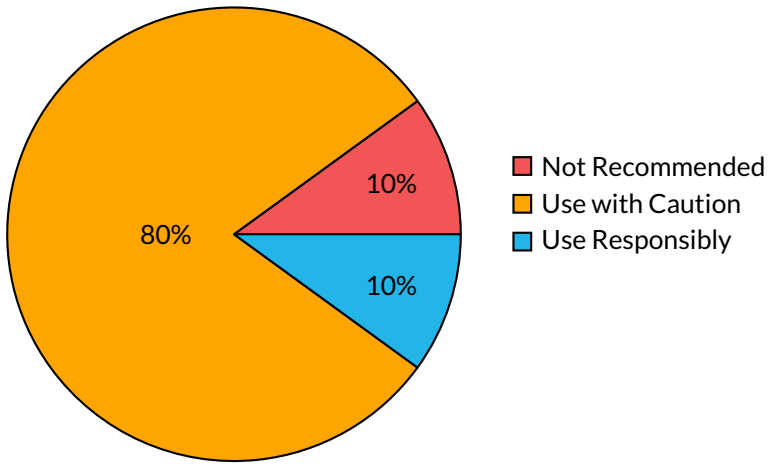


Figure 1: This chart illustrates the breakdown of applications and services receiving each respective tier designation.

7 Common Sense Media, *Information Privacy Updates* (Feb. 2018), https://www.commonsense.org/education/privacy/blog/information-privacy-updates-february-2018.

Use Responsibly

Figure 2: Use Responsibly tier icon.

Applications and services in the "Use Responsibly" tier have met a minimum criteria for transparency and quality in their policies. Before using an application or service in this tier, parents, teachers, schools, and districts are strongly advised to read the full privacy evaluation as a starting point for the process of vetting the service. In addition, a more detailed review should happen before any child or student data is shared with a service. Among the applications and services we evaluated, approximately 10 percent are designated Use Responsibly, which indicates their policies are sufficiently transparent and they provide qualitatively better responses to the Use with Caution and Not Recommended criteria.

Use with Caution

Figure 3: Use with Caution tier icon.

Applications and services in the "Use with Caution" tier have issues narrowly focused around data uses related to creating profiles that are not associated with any educational purpose and/or using data to target advertisements. We include data use from both the first party (i.e., the vendor that builds the service) and third parties (any company given access to data by the vendor). Using data to profile students can potentially violate multiple state laws and, in some cases, federal law.

An application or service can be designated Use with Caution either for a lack of transparency around data use — which creates the potential for profiling and behavioral targeting — or for clearly stating the service uses data to target advertisements and/or create profiles. As with any application being considered for use within schools, school and/or district staff should review the privacy policies and terms of service to ensure that they meet the legal and practical requirements of their state laws and school policies. The questions listed below trigger inclusion in the Use with Caution tier:

1. As discussed in the Effective Date section: Do the policies clearly indicate the version or effective date of the policies?

2. As discussed in the Data Sold section: Do the policies clearly indicate whether or not a user's personal information is sold or rented to third parties?
3. As discussed in the Third-Party Marketing section: Do the policies clearly indicate whether or not personal information is shared with third parties for advertising or marketing purposes?
4. As discussed in the Behavioral Advertising section: Do the policies clearly indicate whether or not behavioral or contextual advertising based on a child or student's personal information is displayed?
5. As discussed in the Third-Party Tracking section: Do the policies clearly indicate whether or not third-party advertising services or tracking technologies collect any information from a user of the application or service?
6. As discussed in the Track Users section: Do the policies clearly indicate whether or not a user's personal information is used to track and target advertisements on other third-party websites or services?
7. As discussed in the Ad Profile section: Do the policies clearly indicate whether or not the vendor allows third parties to use a student's data to create a profile, engage in data enhancement or social advertising, or target advertising to students, parents, teachers, or the school?

An evaluation designation of "Use with Caution" is not a sign that a vendor is doing anything unethical, but it could mean, based on how the application or service is used, that it may be violating either federal or state laws. It is a sign that, based on publicly available policies, we do not have adequate guarantees that data will not be used by first or third parties to create noneducational profiles or to target behavioral ads. The majority of applications and services, approximately 80 percent, are designated "Use with Caution." This high percentage is attributable to general non-transparency as well as qualitatively worse responses to most of the "Use with Caution" criteria. In particular, a majority of applications and services disclosed an effective date or version number of the policies. In addition, a majority of applications and services disclosed that they do not rent, lease, trade, or sell data. However, a majority of applications and services are non-transparent or explicitly allow third-party marketing, behavioral advertising, third-party tracking, tracking users across other websites, or the creation of ad profiles.

Not Recommended

Figure 4: Not Recommended tier icon.

Applications and services in the "Not Recommended" tier have issues narrowly focused on whether a detailed privacy policy is available for evaluation and whether collected information is protected with default encryption during login or account creation to protect child and student data. The questions listed below trigger inclusion in the Not Recommended tier:

1. Is a privacy policy available?
2. Do the account-creation page, the login page, and all pages accessed while a user is logged in *support* encryption with HTTPS?
3. Do the account-creation page, the login page, and all pages accessed while a user is logged in *require* encryption with HTTPS?

The criteria for Not Recommended measure whether or not a vendor has done the bare minimum to provide users with a rudimentary understanding of how the vendor protects user privacy. The three criteria above all are basics of sound privacy and security practice. Applications and services that do not meet these basic requirements can potentially run afoul of federal and state privacy laws.

Nonetheless, as with the Use with Caution criteria described above, a Not Recommended designation is not a sign that a vendor is doing anything unethical, but it could mean, based on how the application or service is used, that it's violating either federal or state laws. It is a sign that, based on publicly available policies and observable security practices, their services do not provide adequate guarantees that information stored in their information systems will be protected. Among the applications and services we evaluated, approximately 10 percent are designated Not Recommended, which indicates their policies are neither sufficiently transparent nor provide qualitatively better responses to the Not Recommended criteria. Among the applications or services we evaluated, each had a privacy policy and/or terms of service available on their website at the time of our evaluation. However, the applications and services designated Not Recommended all failed to protect collected information from children and students with default encryption during the login or account-creation process.

Evaluation Scores

The privacy-evaluation process for an application or service is unique, because it produces two independent scores for transparency and quality, which are combined into an overall score. These two metrics allow for an objective comparison between applications and services based on how transparent their policies are in explaining their practices and the quality of those practices. Other privacy policy assessment tools have used machine learning or algorithmic qualitative keyword-based contextual methods that attempt to summarize a policy's main issues. These machine-learning or keyword-based methods, such as the Usable Privacy Policy Project, have been found to produce reliable measures of transparency information about the key issues disclosed in an application or service's policies. However, these methods are not able to capture substantive indicators that describe the meaning or quality of those disclosures. Therefore, our privacy-evaluation process was developed with this limitation in mind to incorporate both qualitative and quantitative assessment methods to capture the differential meaning of each privacy practice disclosed in a vendor's policies with scores.[8]

Score Calculations

The privacy-evaluation process incorporates over 150 questions into a framework that produces three complementary scores that allow for the objective comparison among applications or services based on transparency, quality, and an overall score. Only questions that are deemed pertinent or expected to be disclosed for the application or service, based on its intended use and context, are used in calculating each score. Questions are expected to be answered based on the intended use of the application or service and the applicable laws governing that intended use, as well as responses to other evaluation questions, which is further explained in the Mapping Compliance section. Given the intended use of the application or service, not answering expected questions negatively impacts that application or service's transparency score and subsequent overall score.

For the evaluation process, "transparency" is defined as a measure indicating, of the things we expect to know, what percentage are knowable. In addition, "quality" is

8 Common Sense Media, *The Privacy Evaluation Numerical Roll-Up Score* (2018), https://www.commonsense.org/education/blog/the-privacy-evaluation-numerical-roll-up-score.

defined as a measure indicating, of those things we know about, whether the vendor's disclosure about those practices protects student information, which is considered qualitatively better. To determine the overall score, we weight the transparency score more heavily to encourage higher levels of transparency, and then we subtract a fractional value of the qualitatively worse responses. This fractional value of the qualitative responses is used to ensure that answering a relatively small number of questions does not disproportionately impact the overall score. In other words, since the quality score is reflective of only those questions that are transparent, we take into consideration that the qualitatively worse responses should only diminish the overall score by an amount reflective of how transparent the policies are. The calculation is then normalized to a 0–100 scale.

The actual equation to calculate the overall score is as follows:

$$\frac{W \times T - \frac{B \times T}{100}}{W}$$

W represents the transparency weight, *T* is the transparency score, and *B* is 100 minus the quality score representing qualitatively worse responses. Note that we currently use a transparency weight (*W*) of 1.2.

Score Examples

For instance, using our equation above, let's examine six scenarios with similar transparency and quality scores that should hopefully illustrate the impact of our overall scoring methodology.

First we will highlight the equation in use by using Scenario 2 to illustrate the overall score calculation. For Scenario 2 we have the following values: *T*=70, and *B*=100-80=20, and the constant transparency weight *W*=1.2.

SCORING METHODOLOGY SCENARIOS

$$Overall = \frac{W \times T - \frac{B \times T}{100}}{W} = \frac{1.2 \times 70 - \frac{20 \times 70}{100}}{1.2} \approx 58.33$$

Scenario	Transparency	Quality	Overall
Scenario 1	70	100	70
Scenario 2	70	80	58.33
Scenario 3	70	50	40.83
Scenario 4	50	100	50
Scenario 5	50	80	41.66
Scenario 6	50	50	29.16

Table 1: This table illustrates different scenarios that impact the overall scoring methodology.

These six scenarios should provide some insight into how transparency and quality contribute to an overall score. There are two considerations to keep in mind when viewing the overall score, as some very different applications and services can end up with similar overall scores. First, how much information do we know, and second, of those things we do know, how many things are qualitatively better? The crossover tends to happen in areas where we know little but what we know is relatively good, or we know a lot and what we know is relatively bad. The scoring methodology provides a primary incentive for transparency — in the case of low transparency and qualitatively better practices — because the incentive is to be more transparent in order to increase the overall score. In addition, there is also a secondary incentive for quality in the case of high transparency and qualitatively poor practices, because the incentive is to improve the qualitative nature of the practices in order to increase the overall score. Note that some practices have inherent risk, and therefore it is not expected that all vendors will achieve a perfect quality score.

Digging into the scenarios, we can see generally that higher transparency results in a higher score. This supports our goal of helping people make informed decisions. As the number of qualitatively better responses diminishes, even high transparency is not sufficient to maintain a high overall score, and in the case of Scenario 3 (which has relatively high transparency with relatively lower quality scores), we see that it dips below Scenario 5 (which has lower transparency but higher quality scores). This may seem counterintuitive, but at a glance both scores, 40.83 and 41.66 respectively, indicate that a fair amount of additional work is necessary in order to use the respective application in a safe manner. It is our hope that the overall score is a useful approximation of the amount of additional work necessary to use each application or service safely.

Figure 5 illustrates the interaction of quality and transparency in the overall score. Each color band represents an overall score within a five-point range. The bottom-left contour represents those applications and services receiving an overall score in the range of 0 to 5, whereas the top-right-most contour represents those policies receiving an overall score of 95 to 100. As you can see, higher overall scores are more difficult to achieve and represent a narrower type of application or service. This scale allows for more differentiation in those policies that have met a sufficient transparency and qualitative threshold. From a quick glance, this threshold starts to happen somewhere in the range of 50–100, which is expected, as policies below that threshold are not transparent enough and/or have insufficient qualitatively better responses.

The area under the contour line indicates the relative amount of information that you do know and that you know is qualitatively better about a set of policies. It is increasingly difficult to know everything about an application or service and have everything you know be qualitatively better. It is our opinion that vendors in the edtech industry especially should be striving for excellence in providing qualitatively better practices. As such, our overall scoring methodology sets a high expectation.

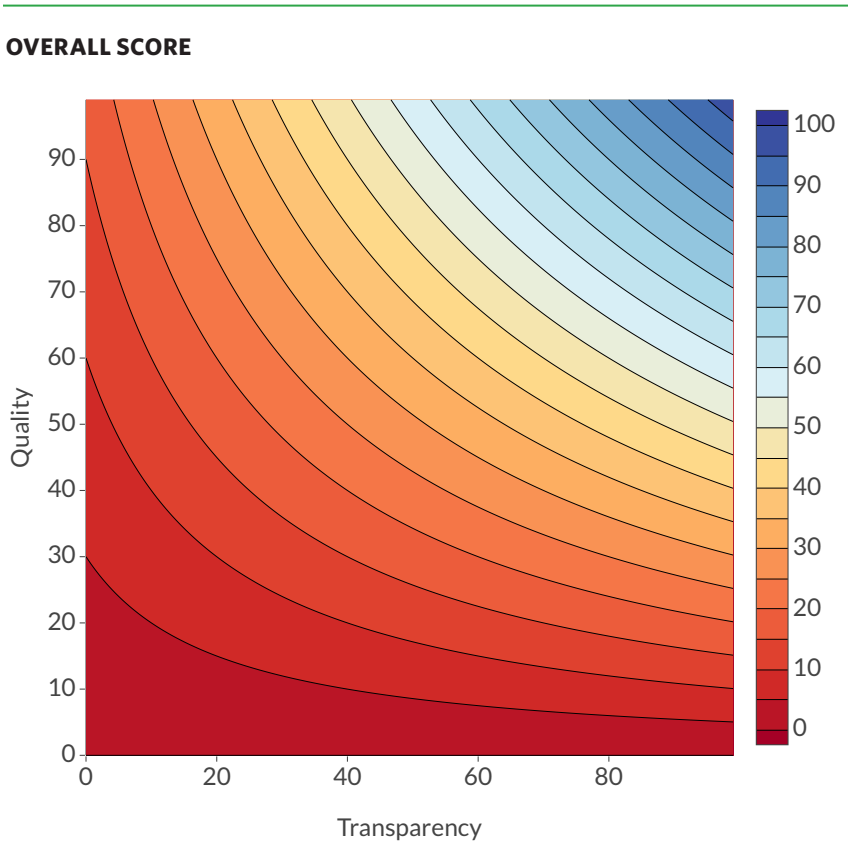


Figure 5: This chart illustrates the interaction of quality and transparency in the overall score.

Determining Transparency

Among all applications and services evaluated, our analysis determined that approximately only 48 percent of all questions received transparent responses. This finding is lower than expected, given that this means applications and services are only providing transparent responses to approximately half of all our evaluation questions. This behavior likely can be explained by the common practice of vendors attempting to limit their potential liability by not making promises they are not legally required to disclose in their policies, thereby not disclosing potentially qualitatively worse practices. In addition, lower-than-expected transparency also is likely attributable to vendors not disclosing qualitatively worse practices that they do not engage in, or not having sufficient resources or legal advice when crafting their own policies. Low transparency in our evaluation process could also be attributed to privacy issues where a vendor has a legal compliance requirement, but there is not a corresponding legal requirement to affirmatively disclose the respective details of compliance. Lastly, the lower-than-expected transparency findings are consistent with further analysis that indicates a similar overall transparency mean for all applications and services evaluated of approximately 60/100.

TRANSPARENT VERSUS NON-TRANSPARENT RESPONSES

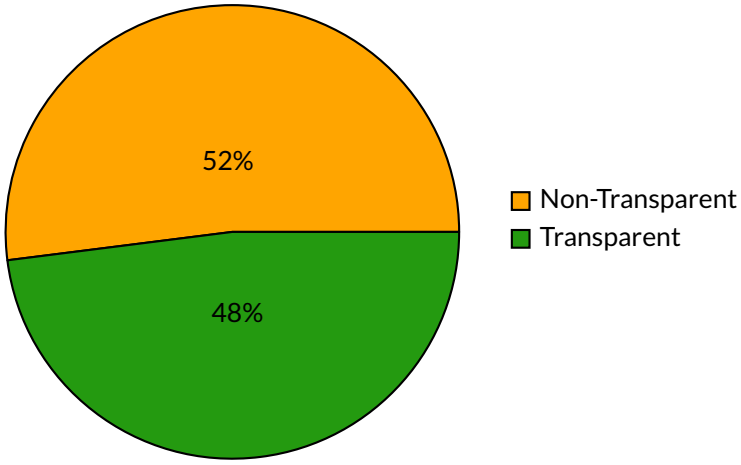


Figure 6: This chart illustrates the percentage of question responses indicating that the terms are transparent about whether or not the application or service engages in the practice specified in each evaluation question versus those that are non-transparent.

Determining Quality

Some questions also have a qualitative component that aims to capture the better or worse nature of the practice. For these questions that have transparent disclosures, there is an objectively better answer of quality. This relative difference in quality is important, because practices are inherently better or worse depending on the context in which they are used. If an application or service does not disclose it engages in practices that are better for privacy, the quality score will be negatively impacted. Given that the context in which an application or service could be used varies, not all questions are weighted the same in our calculations. Depending on the questions expected to be answered, individual question weights are dynamic, as explained later in the report. Among all applications and services evaluated, our analysis determined that among the approximately 48 percent with transparent disclosures, approximately 62 percent of questions received qualitatively better responses. This finding is important, given that these applications and services are already transparent, and therefore their disclosures are more likely qualitatively better. In addition, this finding also is consistent with further analysis that indicates a similar overall quality mean of 67/100. However, this finding raises further questions as to why such a high percentage of applications and services, approximately 38 percent, discloses qualitatively worse practices. Further analyses in this report attempt to deconstruct these findings and provide answers to why questions are more likely to receive qualitatively better or worse responses.

QUALITATIVELY BETTER VERSUS QUALITATIVELY WORSE RESPONSES

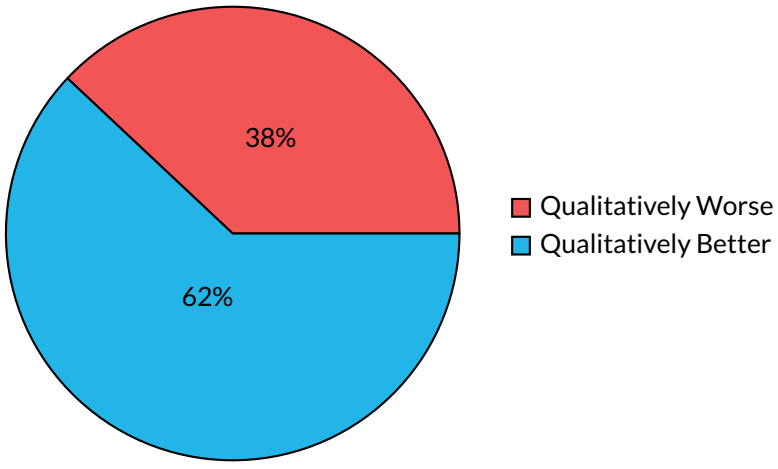


Figure 7: This chart illustrates the percentage of question responses indicating a qualitatively better response versus those receiving qualitatively worse responses.

Determining Weight

Each question is assigned one of five weight categories (very low, low, medium, high, very high). The combination of all questions in each weight category contributes the following percentage to an application or service's score:

- Very low: 5 percent
- Low: 10 percent
- Medium: 20 percent
- High: 30 percent
- Very high: 35 percent

Each expected question with a transparent response contributes one point to its respective weight category for transparent responses. These points are then divided by the number of expected questions in the corresponding weight category to obtain the weight category score. Each weight category score is then multiplied by the respective category weight, and these values are summed to obtain the overall weighted score. An example will help illustrate this weighting process, assuming the question breakdown and transparent responses as seen in Table 2.

QUESTION WEIGHT SCENARIOS

Weight Category	Expected Questions	Transparent Responses	Raw Score	Category Weight	Weighted Score Contribution
Very Low	10	7	0.7	5	3.5
Low	20	15	0.75	10	7.5
Medium	40	27	0.675	20	13.5
High	20	17	0.85	30	25.5
Very High	10	5	0.5	35	17.5

Table 2: This table illustrates different question weight scenarios that impact the overall scoring methodology.

An unweighted transparency score would be 71/100 (100 questions, 71 transparent). A weighted score would be 67.5/100, where each category contributes the following points:

- Very Low: 3.5 (0.7 x 5)
- Low: 7.5 (0.75 x 10)
- Medium: 13.5 (0.675 x 20)
- High: 25.5 (0.85 x 30)
- Very High: 17.5 (0.5 x 35)

The same weighting process is applied to quality scores with the only exception being that we only consider those questions that have a qualitative component and are transparent. This process minimizes the potential of penalizing an application or service for not addressing evaluation questions that are not relevant. If a weight category has no questions expected to be answered, then the total score is curved as though that weight category did not exist (e.g., if no questions in the "Very High" category are expected to be answered, then the score would be calculated against a total possible 65 [100 - 35] rather than 100). Weighting evaluation questions is appropriate given the non-conforming nature of the question set, where questions expected to be answered fall across a broad spectrum.

Determining the weight for each question is based on several factors that include: objective statutory or regulatory requirements, our subjective expertise in this subject matter, contextual relevance, and industry best practice. Evaluation question responses can be expected to be disclosed as a matter of law, because disclosure provides users with adequate notice in which to give their informed consent. For example, applications and services are required to provide notice of the effective or revision dates of their privacy policies. Evaluation questions also can be expected to be disclosed as a matter of context, given how the application or service is intended to be used. For example, if an application or service is intended to be used by children or students under 13 years of age, then notice is required to be provided about obtaining verifiable parental consent. Lastly, evaluation questions also can be expected to be disclosed if they are considered standard industry best practice. For example, disclosure that reasonable security practices are provided to protect collected information would be considered a standard industry best practice in which to protect child and student data.

DISTRIBUTION OF WEIGHT CATEGORIES

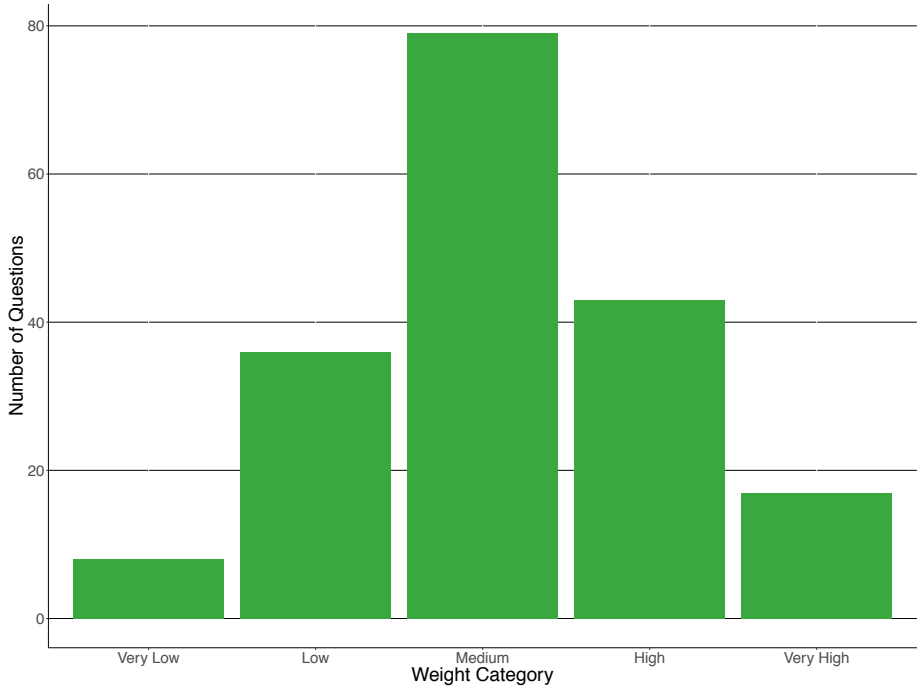


Figure 8: This chart illustrates the frequency distribution of evaluation question weight.

Mapping Compliance

The privacy-evaluation process includes mapping over 150 statutory and regulatory requirements to the privacy evaluation question framework with parenthetical citations explaining each citation's requirements in plain English.[9] These citations cover both federal and state law and allow the categorization of evaluation questions into different sections for each applicable statute or regulation. These legal sections illustrate the interdependent relationships among the evaluation questions themselves, and also indicate relative compliance scores for each law. These statute scores are differentiated from transparency, quality, and overall scores in that they do not use expected- or not-expected-to-be-disclosed distinctions in calculating the score, because the questions that pertain to that specific law are treated as expected to be answered.

To graphically illustrate these relationships, each question is represented by a two-word description label around the outside of the radial graph (see Figure 9). The relationships among all questions are shown by connected lines between each two-word description that represent shared legal obligations of both federal and state law. An

9 Common Sense Media, *Navigate the Privacy Evaluation Questions*, https://www.commonsense.org/education/privacy/questions/navigate-by-category.

interactive version of this radial graph with more examples is available at https://privacy.commonsense.org/question-dependency.

QUESTION COMPLIANCE RELATIONSHIPS

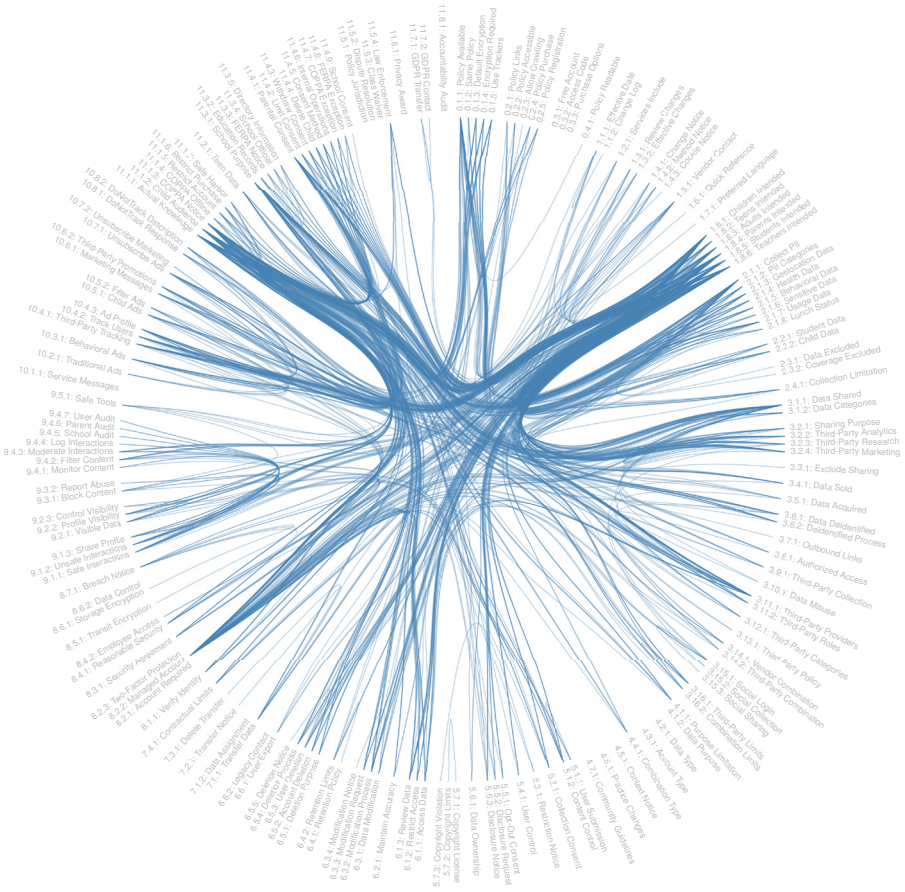


Figure 9: This chart illustrates mapping compliance relationships through a radial graph.

In the interactive version of this radial graph, any two-word description on the outside can be selected and will appear in black. When a question is selected, some are highlighted in green or red. A green link indicates a "parent" relationship. A red link indicates a "child" relationship. Child links to questions are dependent upon the question you have selected, because they require your selected question to be answered first before they can be answered. Parent links to questions are dependencies for other questions that require that they be answered before your selected question. In the interactive version, once a question is selected, you can see green parent links to other questions that would need to be answered beforehand. In addition, you can also see red children links to other questions that indicate that if the selected question is required to be answered, then those questions that share the same legal obligations will also be required.

Table 3 illustrates all the statutory and regulatory laws that are mapped to the evaluation framework and the frequency of questions that reference that specific law.[10]

QUESTION COMPLIANCE REFERENCES

Statute	Name	Frequency
Children's Online Privacy Protection Act (COPPA)[11]	COPPA	79
Student Online Personal Information Protection Act (SOPIPA)[12]	SOPIPA	39
Family Educational Rights and Privacy Act (FERPA)[13]	FERPA	38
California Online Privacy Protection Act (CalOPPA)[14]	CalOPPA	29
California AB 1584 - Privacy of Pupil Records (AB 1584)[15]	AB 1584	17
California Privacy Rights for Minors in the Digital World (CalPRMDW)[16]	CalPRMDW	12
California Privacy of Pupil Records (CalPPR)[17]	CalPPR	8
California Data Breach Notification Requirements (DataBreach)[18]	DataBreach	6
General Data Protection Regulation (GDPR)[19]	GDPR	4
Children's Internet Protection Act (CIPA)[20]	CIPA	4
Early Learning Personal Information Protection Act (ELPIPA)[21]	ELPIPA	4
Protection of Pupil Rights Act (PPRA)[22]	PPRA	3
The Communications Decency Act of 1996 (CDA)[23]	CDA	3
California "Shine the Light" (ShineTheLight)[24]	ShineTheLight	2
California Electronic Communications Privacy Act (CalECPA)[25]	CalECPA	2
Digital Millennium Copyright Act (DMCA)[26]	DMCA	2
Copyright Act of 1976 (Copyright)[27]	Copyright	2
The National School Lunch Act (NSLA)[28]	NSLA	1
California Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)[29]	RUFADAA	1
California Electronic Commerce Act (CalECA)[30]	CalECA	1
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003[31]	CAN-SPAM	1

Table 3: This table illustrates the frequency of statutory and regulatory laws that reference questions.

10 Common Sense Media, *Privacy Evaluation Visualization*, https://privacy.commonsense.org/question-dependency.

11 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.

12 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584.

13 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1.

14 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575.

15 California AB 1584 Privacy of Pupil Records, Cal. Ed. Code §§49073.1.

16 California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§22580-22582.

17 California Privacy of Pupil Records, Cal. Ed. Code §49074.

18 California Data Breach Notification Requirements, Cal. Civ. Code §1798.29.

The evaluation framework distributes these statutes and regulations across all evaluation questions with the majority of questions having more than one relevant federal or state law associated with the issues raised in that question. Figure 10 illustrates that most evaluation questions reference laws associated with protecting information collected from children and students through the Children's Online Privacy Protection Act (COPPA), the Student Online Personal Information Protection Act (SOPIPA), and the Family Educational Rights and Privacy Act (FERPA).

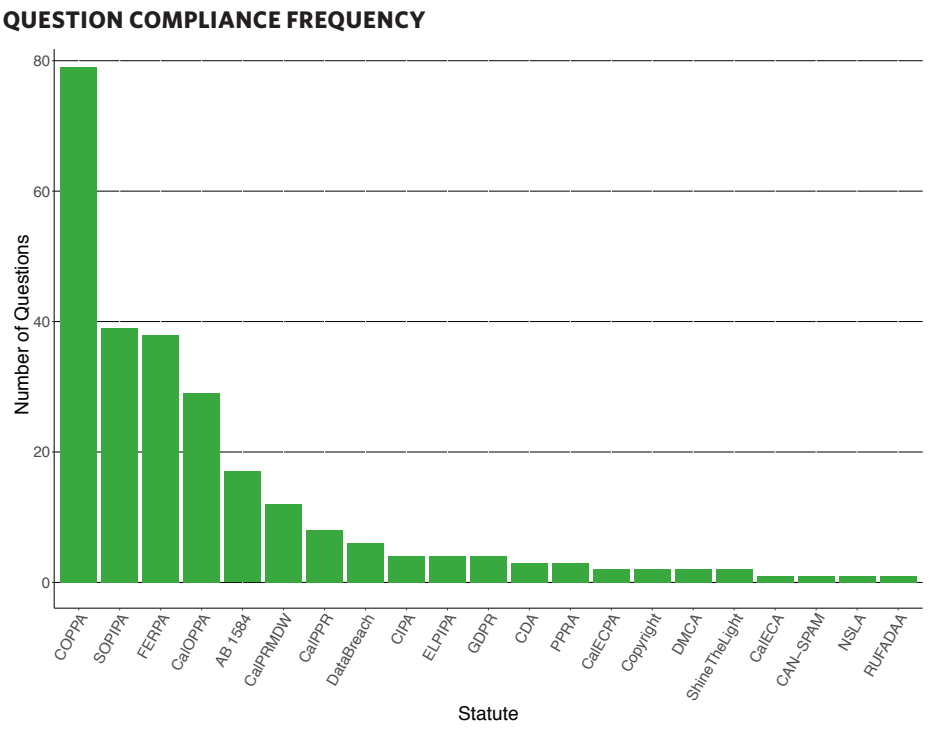


Figure 10: This chart illustrates the frequency of evaluation questions that reference specific laws.

19 General Data Protection Regulation (GDPR), (Regulation (EU) 2016/679).

20 Children's Internet Protection Act (CIPA), 47 U.S.C. §254.

21 Early Learning Personal Information Protection Act (ELPIPA), Cal. B.&P. Code §22586.

22 Protection of Pupil Rights Act (PPRA), 34 C.F.R. Part 98.

23 The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(d).

24 Information Sharing Disclosure, Cal. Civ. Code §§1798.83-1798.84.

25 California Electronic Communications Privacy Act, Cal. Pen. Code §1546-1546.4.

26 Digital Millennium Copyright Act (DMCA), 17 U.S.C. §512(g)(2)(A).

27 Copyright Act of 1976, 17 U.S.C. §102.

28 The National School Lunch Act (NSLA), 42 U.S.C. §§1751-63.

29 California Revised Uniform Fiduciary Access to Digital Assets Act, Cal. Prob. Code §870-884.

30 California Electronic Commerce Act, Cal. Civ. Code §1789.3.

31 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 16 C.F.R. Part 316.5.

RESULTS

Normal Distributions

The following normal distributions illustrate the overall transparency, overall quality, and overall scores of 100 popular edtech applications and services. Each chart also includes a Tukey box plot at the top to help readers understand the distribution of the scores, with lower quartile (Q1), median (Q2), upper quartile (Q3), and whiskers indicating the lowest and highest datum within 1.5 times the interquartile range IQR(Q3–Q1), and values falling outside 1.5 times the IQR are considered outliers and denoted with circles. The table below summarizes our findings for transparency, quality, and overall score.

SCORING SUMMARY STATISTICS

Score Type	Min.	Mean	$Q1$	Median($Q2$)	$Q3$	Max.	Stdev
Transparency	17	60	52	63	70	94	16
Quality	39	67	61	69	75	87	10
Overall	11	44	37	43	52	75	13

Table 4: This table illustrates summary statistics for transparency, quality, and overall score.

Overall Transparency Normal Distribution

Among the applications and services evaluated, Figure 11 illustrates an overall transparency score range from a minimum of 17 to a maximum of 94, with a mean of 60/100 and a standard deviation of 16. This distribution is expected given our earlier analysis that approximately 48 percent of all questions received transparent responses.

TRANSPARENCY SCORE

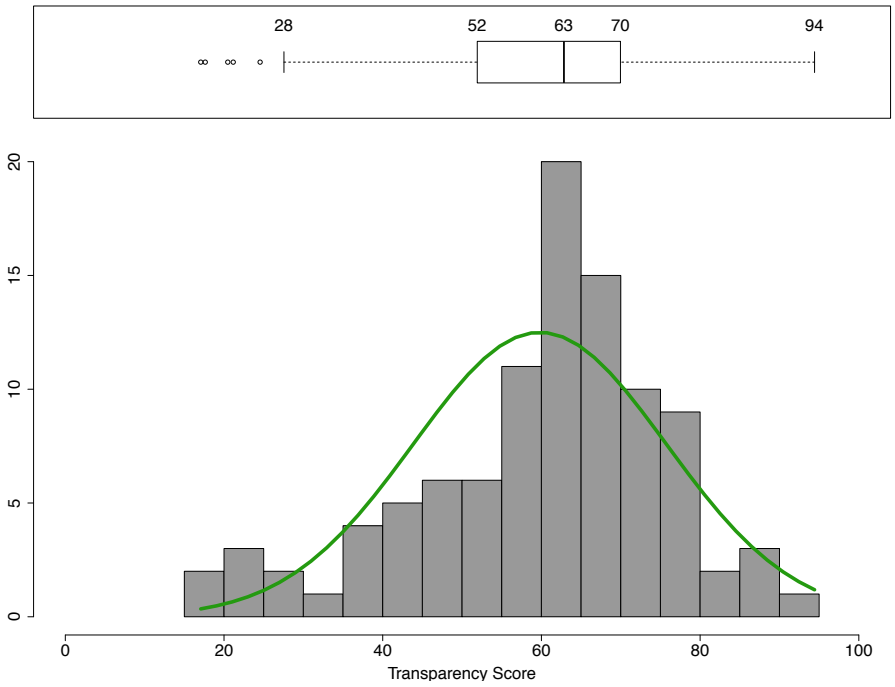


Figure 11: This chart illustrates the transparency score distribution histogram and normal curve, with median (Q2) 63, lower quartile (Q1) 52, upper quartile (Q3) 70, lower whisker 28 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 94 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Overall Quality Normal Distribution

Among the applications and services evaluated, Figure 12 illustrates an overall quality score range from a minimum of 39 to a maximum of 87, with a mean of 67/100 and a standard deviation of 10. This skewed distribution of results greater than 50 is expected given our earlier analysis that approximately 62 percent of all questions received qualitatively better responses.

QUALITY SCORE

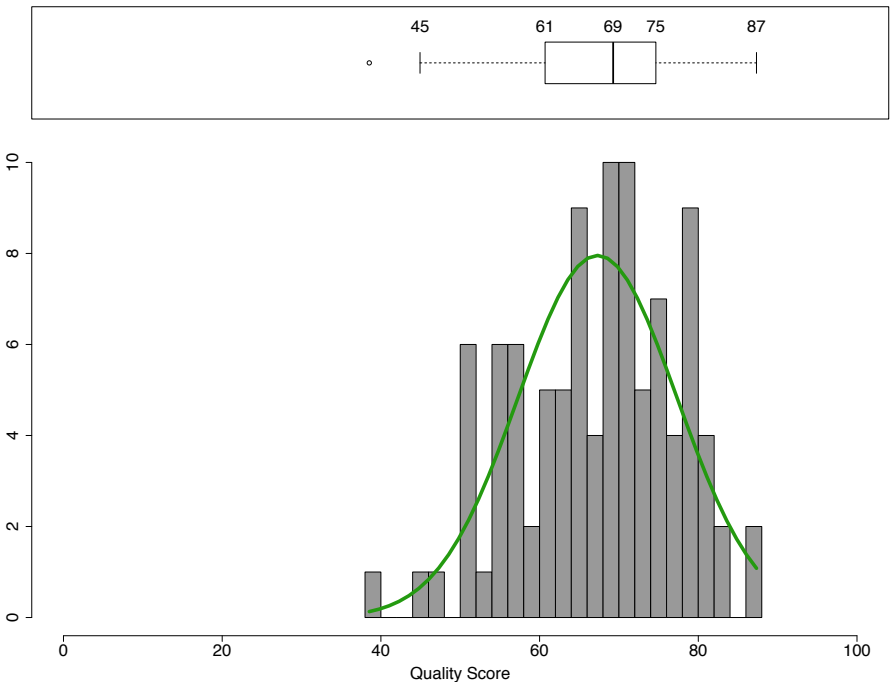


Figure 12: This chart illustrates the quality score distribution histogram and normal curve, with median (Q2) 69, lower quartile (Q1) 61, upper quartile (Q3) 75, lower whisker 45 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 87 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Overall Score Normal Distribution

Among the applications and services evaluated, Figure 13 illustrates an overall numerical roll-up score range from a minimum of 11 to a maximum of 75, with a mean of 44/100 and a standard deviation of 13. With an overall score mean of 44/100, most applications and services evaluated have significant deficiencies in both transparency and qualitatively better disclosures for privacy and security practices. With overall scores upper-bound by transparency, our analysis determined that an overall lack of transparency and lack of qualitatively better disclosures across all evaluation questions contributed heavily to the lower mean.

OVERALL SCORE

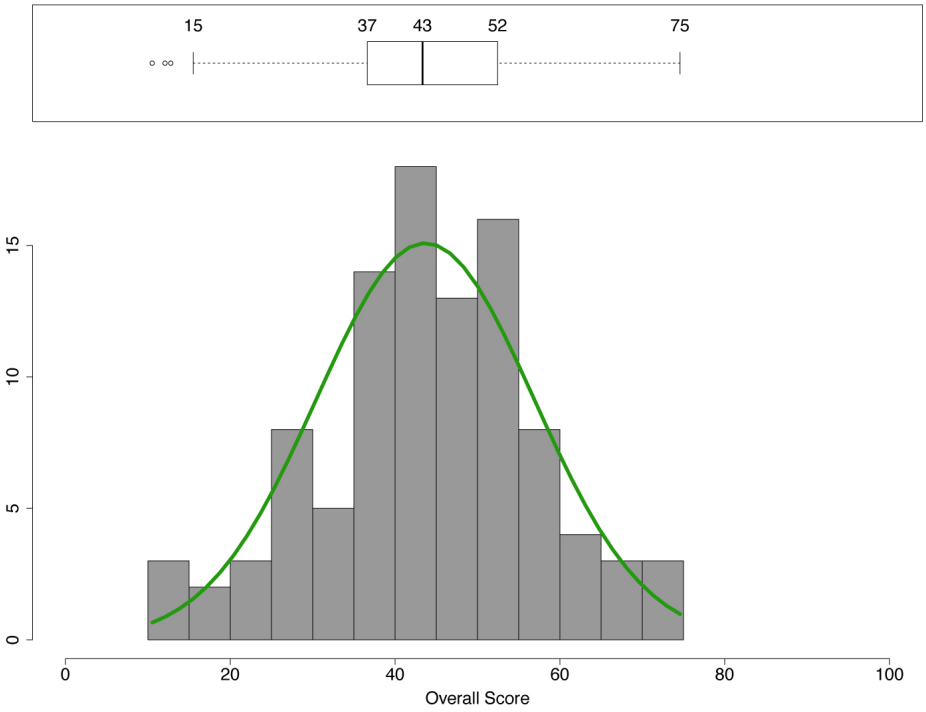


Figure 13: This chart illustrates the overall score distribution histogram and normal curve, with median (Q2) 43, lower quartile (Q1) 37, upper quartile (Q3) 52, lower whisker 15 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 75 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Regression Analysis

Overall Transparency and Overall Quality

In this comparison between the overall transparency and overall quality scores for an application or service, quality is not upper bound by the weighted percent transparent. In addition, non-transparent responses in this analysis do not indicate a qualitatively better or worse response, and therefore are not reflected in an application or service's overall quality score. From the regression below, you can see that as transparency increases, the standard deviation of quality decreases. That is, higher transparency results in a lower variance in quality. This relationship is partially expected given our previous findings that indicated a correlation between transparency and disclosure of qualitatively better practices. A lower transparency score means a lower representation across all questions, but disclosure on a single question can skew the results heavily, because as transparency increases, there is more information available in which to make a better informed and reliable assessment of quality. This is a strong indicator,

among those services evaluated, that, barring any other information, transparency is a reliable proxy for quality. In addition, as transparency increases above specific thresholds, the reliability of the overall score increases; you can see this in the "funnelling effect" as the values progress to the right.

OVERALL TRANSPARENCY VERSUS QUALITY

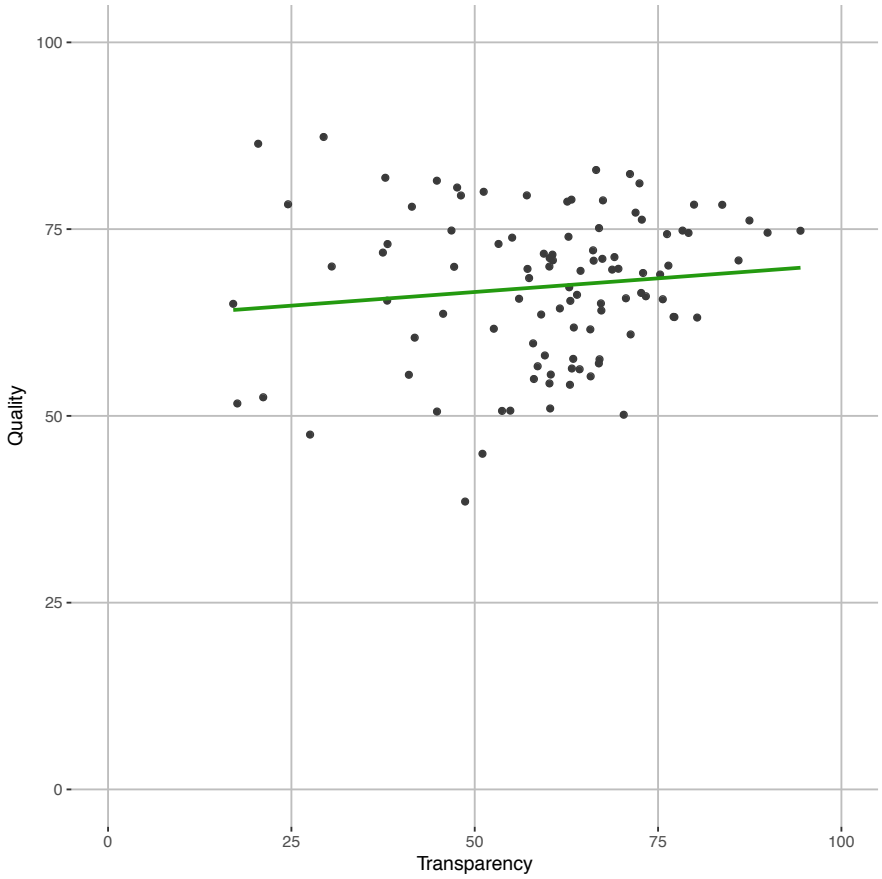


Figure 14: This chart illustrates the transparency and quality score distribution. Note that as transparency increases, the spread of quality scores becomes narrower.

Statute Scores

Each statute or regulation is associated with one or more evaluation questions. As discussed, statute scores are differentiated from transparency, quality, and overall scores in that they do not use expected- or unexpected-to-be-disclosed distinctions in calculating the score, because the questions that pertain to that specific law are treated as expected to be answered. This strict compliance evaluation process means that each question's transparency and qualitative response serves as an indirect proxy for that specific law's transparency, quality, and overall score, which indicate the likelihood of

the application or service satisfying its compliance obligations. For example, all evaluation questions that reference the Children's Online Privacy Protection Act (COPPA) would be expected to be disclosed and used to calculate statute-specific scores for transparency, quality, and an overall score that indicate an application or service's likelihood of compliance under COPPA.[32]

COPPA Transparency Normal Distribution

Figure 15 illustrates the COPPA transparency score range from a minimum of 7 to a maximum of 93, with a mean of 60/100 and a standard deviation of 19. Given that the majority of applications and services evaluated are intended for children under 13 years of age, this finding is lower than expected but should also take into account several outliers below 25 that lower the overall mean. However, lower COPPA transparency scores are likely attributable to applications and services that disclose they are not intended for children under 13 years of age.

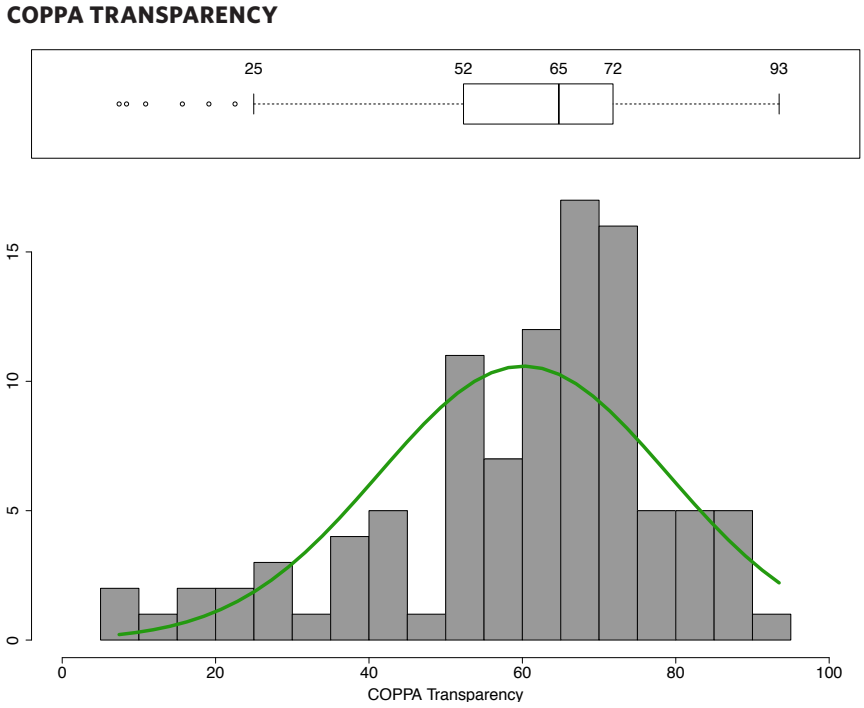


Figure 15: This chart illustrates the COPPA transparency score distribution histogram and normal curve with median (Q2) 65, lower quartile (Q1) 52, upper quartile (Q3) 72, lower whisker 25 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 93 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

32 *See supra* note 11.

COPPA Quality Normal Distribution

Figure 16 illustrates the COPPA quality score range from a minimum of 20 to a maximum of 88, with a mean of 65/100 and a standard deviation of 13. This distribution of higher-quality results is expected, given that if applications and services are transparent about COPPA-related compliance issues, they are likely to disclose qualitatively better responses regarding their practices being in compliance with the law.

COPPA QUALITY

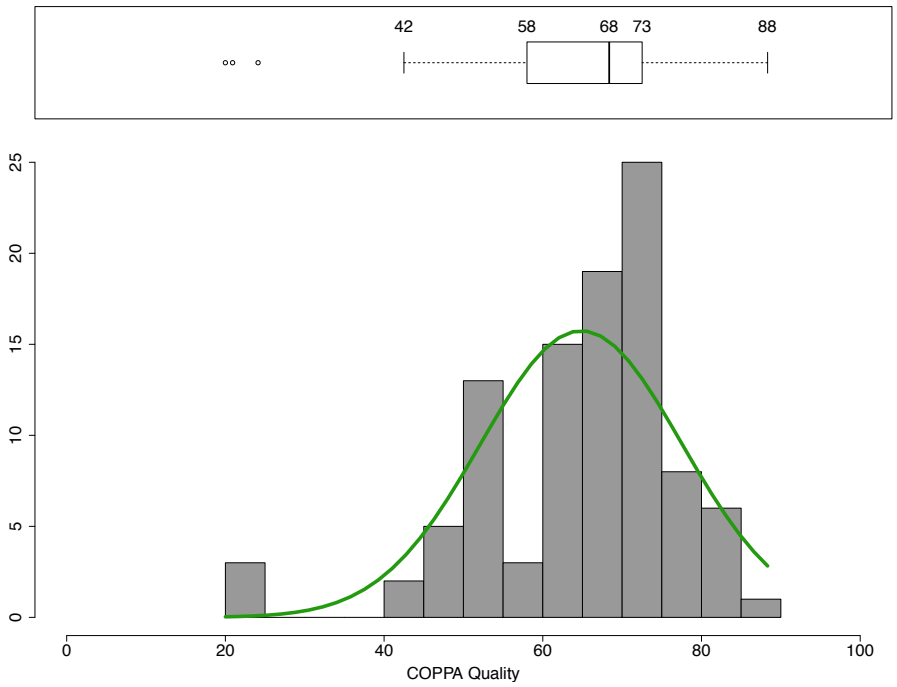


Figure 16: This chart illustrates the COPPA quality score distribution histogram and normal curve with median (Q2) 68, lower quartile (Q1) 58, upper quartile (Q3) 73, lower whisker 42 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 88 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

COPPA Overall Score Normal Distribution

Figure 17 illustrates the COPPA overall score range from a minimum of 3 to a maximum of 78, with a mean of 43/100 and a standard deviation of 16. As discussed, given that the majority of applications and services evaluated are intended for children under 13 years of age, this lower-than-expected COPPA overall score mean indicates vendors still need to improve their transparency and qualitative disclosures to demonstrate compliance with the law. A lower overall score for an application or service means too

much additional work is required on the part of parents, teachers, schools, and districts to determine whether an application or service is in compliance for their context.

COPPA OVERALL

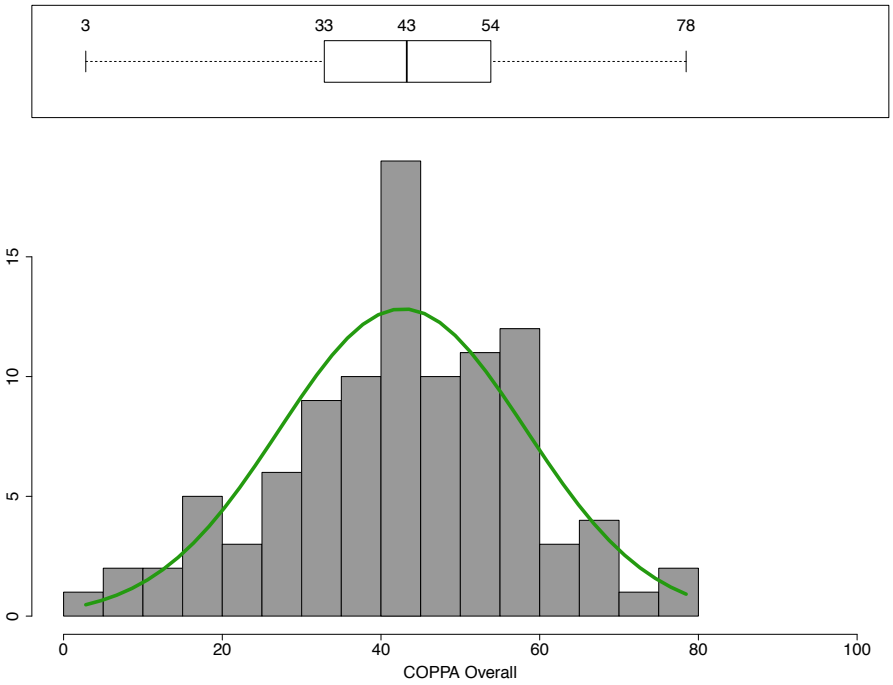


Figure 17: This chart illustrates the COPPA overall score distribution histogram and normal curve with median (Q2) 43, lower quartile (Q1) 33, upper quartile (Q3) 54, lower whisker 3 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 78 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

However, this statute score calculation method only provides an indication of how much additional work is required to determine whether an application or service is actually in compliance with applicable federal or state law in context. Additional information is required to determine whether or not an application or service is compliant in all contexts. A lower score indicates that various use contexts will require more additional work and clarification. A higher score indicates that various contexts will provide the necessary information to determine compliance is satisfied for that particular use. Requiring all statute-specific questions to be expected to be answered provides a score that is an indication across all possible contexts that users can expect to have enough information to make an informed decision. A lower statute overall score indicates that an application or service is more likely to be missing information or clarity with respect to particular details that may be pertinent in a specific context or use case. More work would be necessary to ensure the appropriateness of the application or service in each

particular context. Moreover, each application or service's legal obligations should only be understood in the context in which it is used, and therefore statute scores are not further examined in the results of this report.

Key Findings

The following key findings represent the most important results from our evaluation of 100 popular edtech applications and services. These findings are a representative sample of the most important privacy practices that parents, teachers, and districts have indicated they look for when deciding which application or service to use with their child at home or with students in the classroom. The focus of our key findings are primarily the issues involving advertising and marketing products to children and students. In addition, our key findings include disclosures that child or student information may be used for advertising profiles and tracking users across third-party websites.

The following charts illustrate the results for both transparency and qualitative questions. Transparency questions aim to answer whether or not a policy discloses details with respect to certain practices. Transparency questions can have either transparent or non-transparent results. Qualitative questions aim to answer, given specific practices are disclosed, how the application or service engages in those practices. Qualitative questions can have either qualitatively better or qualitatively worse results. In addition, questions can be either expected- or not-expected-to-be disclosed given the intended use and context of the application or service. Questions that are not expected to be answered may not necessarily require disclosure of that practice in the respective context in which it is used.

Default Encryption

A majority of applications and services use default encryption of information for login and account creation. Among the applications and services we evaluated, approximately 92 percent observationally provided encryption of information collected during the login or account-creation process. This is a notable improvement as compared to our previous login encryption survey findings, which indicate only approximately 74 percent of the more than 1,000 applications or services surveyed support encryption at login.[33] We currently evaluate only encryption of services with login authentication, and not whether encryption is implemented for any authenticated mobile applications. Encryption of login information is expected to be disclosed, because it is an important tool necessary to protect children and student's personal

information online. In addition, approximately 7 percent disclosed not-expected responses. However, approximately 8 percent of applications and services evaluated did not encrypt either their login or account-creation information. Lack of encryption of collected information from children or students in this context is qualitatively worse, because a lack of protection of this information with reasonable security measures would likely violate several federal and state laws. [34, 35, 36, 37, 38]

QUESTION: DEFAULT ENCRYPTION

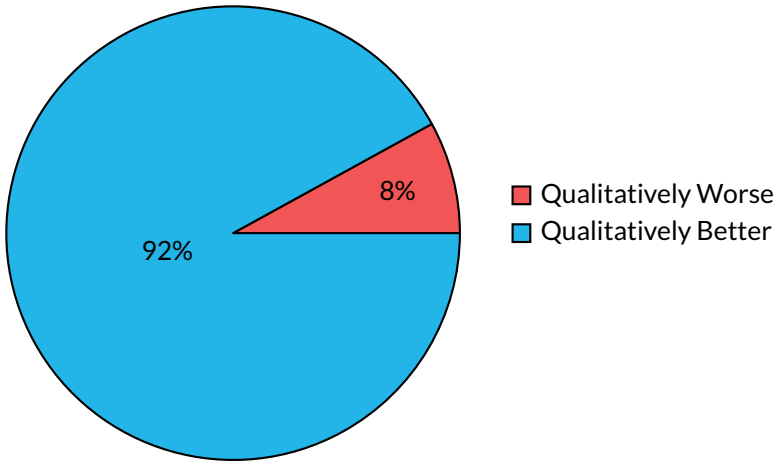


Figure 18: This chart illustrates the percentage of question responses about default encryption. Qualitatively better question responses indicate the application or service does use encryption. Qualitatively worse question responses indicate the application or service does not use encryption.

33 Common Sense Media, *Login Encryption Survey: March 2017* (2017), https://www.commonsense.org/education/privacy/blog/encryption-survey-march-2017.

34 California Data Breach Notification Requirements, Cal. Civ. Code §1798.81.5 (a person or business that owns, licenses, or maintains personal information about a California resident is required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure).

35 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(e) (an operator must maintain the confidentiality, security, and integrity of personal information collected from children).

36 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii) (an educational institution must maintain physical, technical, and administrative safeguards to protect student information).

37 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(d)(1) (an operator is required to implement reasonable security procedures and practices and protect student data from unauthorized access, destruction, use, modification, or disclosure).

38 California AB 1584 Privacy of Pupil Records, Cal. Ed. Code §49073.1(b)(5) (a local educational agency that enters into a contract with a third party must ensure the contract contains a description of the actions the third party will take, including the designation and training of responsible individuals, to ensure the security and confidentiality of pupil records).

Effective Date

A majority of applications and services disclose an effective date or version number of the policies. Among the applications and services we evaluated, approximately 89 percent were transparent and disclosed a version and/or effective date of the policies in compliance with state law.[39] A version or effective date provides notice to consumers of exactly what terms they actually provide their consent to and, more importantly, give notice in the event any changes are made to the policies, requiring a new effective date. However, our evaluation process uncovered that a majority of applications and services with more than one policy often have different effective dates or versions for each policy. Therefore, consumers need to track multiple effective dates against multiple policies, which creates consumer confusion about which policy has changed. It is recommended when an application or service makes substantive changes to a single policy and changes the version or effective date, it should also take the opportunity to review and revise any additional policies in order to have all policies share the same effective date. In addition, it may be easier for applications and services to combine policies if applicable and have all their policies and contractual agreement templates in one place, which would provide parents, teachers, schools, and districts with a single location to find and access all required resources. These best practices would support greater consumer confidence and comprehension when substantive changes are made to multiple policies and ensure all of a product's terms are all up to date.

QUESTION: EFFECTIVE DATE

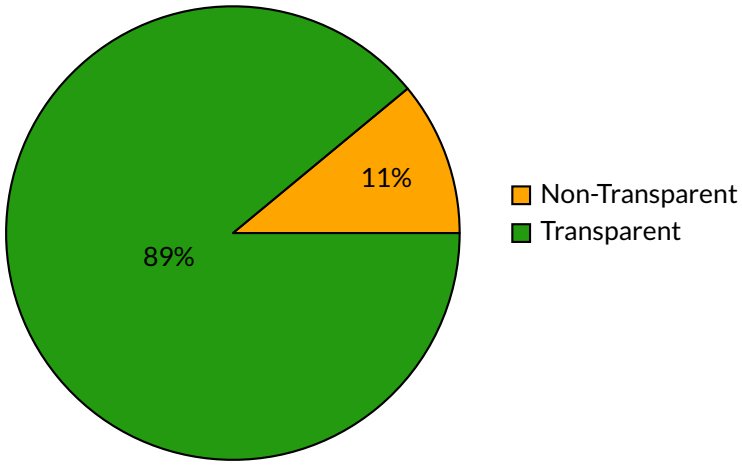


Figure 19: This chart illustrates the percentage of question responses about effective date. Transparent question responses indicate the application or service provides a version or ef-

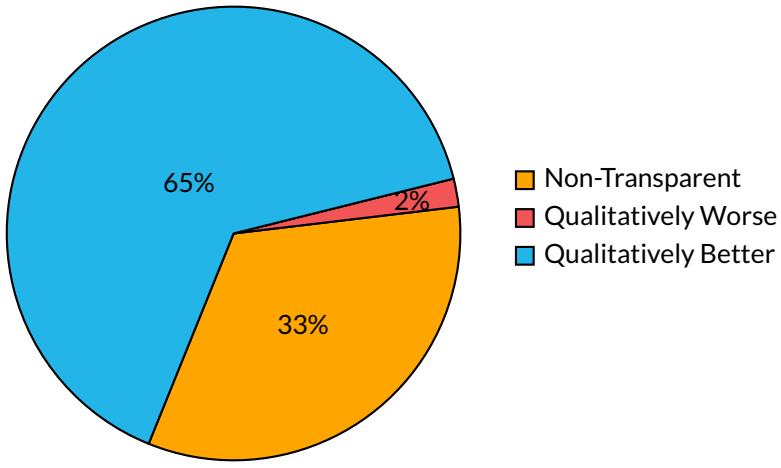
39 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(4) (an operator is required to provide notice of the effective or revision date of its privacy policy).

fective date. Non-transparent responses indicate the application or service does not provide a version or effective date.

Data Sold

A majority of applications and services disclose they do not rent, lease, trade, or sell data, but many are non-transparent. Among the applications and services we evaluated, approximately 65 percent disclosed a qualitatively better response that they do not sell, rent, lease, or trade any users' personally identifiable information to third parties. However, our analysis indicates a large percentage, approximately 33 percent of applications and services evaluated, are non-transparent on this critical issue. Moreover, because both federal and state law clearly prohibits such activities involving children and students, it is assumed a large majority of non-transparent applications and services are in good faith following the law and not selling personal information to third parties but are not disclosing their compliance.[40, 41] Therefore, applications and services need to provide greater transparency on this issue, because they are among the 100 most popular educational technology products, and as indicated in the Children Intended and Students Intended sections, there is a significant percentage of applications and services that disclosed they are intended for children and students but did not also disclose whether they sell, rent, or lease collected personal information. When these practices are not transparently disclosed, there is no future expectation or trust on behalf of parents, teachers, schools, or districts about how collected information from children and students will be handled in order to meet their expectations of privacy.

QUESTION: DATA SOLD



40 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (release of personal information means the sharing, selling, renting, or transfer of personal information to any third party).

41 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(b)(3) (an operator is prohibited from selling or renting student information).

Figure 20: This chart illustrates the percentage of question responses about data sold. Qualitatively better question responses indicate the application or service does not sell any users' personally identifiable information to any third party. Qualitatively worse question responses indicate the application or service may sell any users' personally identifiable information to any third party. Non-transparent responses indicate the terms are unclear about whether or not the application or service sells information to third parties.

Third-Party Marketing

A majority of applications and services are non-transparent or explicitly allow third-party marketing. Among the applications and services we evaluated, approximately 32 percent disclosed a qualitatively better response that collected personal and non-personal information is never used for any third-party marketing purposes. However, approximately 30 percent of applications and services were non-transparent about this practice, ostensibly because many do not display any marketing-related first- or third-party advertisements. Therefore, these applications and services likely believe it to be self-evident that if no marketing advertisements are displayed, then a user's data would not also be used for any unsolicited marketing purposes. When marketing practices are not transparently disclosed, there is no future expectation or trust on behalf of parents, teachers, schools, or districts about how collected information from children and students will be handled in order to meet their expectations of privacy.

However, from a parent or teacher's perspective, there is not any meaningful distinction between the display of advertisements and use of children or student's information for marketing communications. Surprisingly, a relative majority in this analysis of approximately 38 percent of applications and services disclosed they use child or student personal information for advertising or marketing purposes. Given these products are intended for children and students, they are likely in violation of federal or state law if other protections are not put in place.[42, 43, 44, 45] Among the 38 percent of applications and services collecting child or student personal information for advertising or marketing purposes, a majority use language to restrict their use of personal information for marketing purposes to only parent or teachers in order to avoid compliance issues with children or students. However, it is unclear from our analysis how vendors respect the different contexts of acceptable and unacceptable use of collected information for marketing purposes. For example, when personal information is collected from parents and teachers and used for explicit marketing purposes, that is a context different from when personal information is collected for a separate and compliance-related context

of providing parental consent for a child or student's use of the service. Moreover, a combined 68 percent of applications and services were either non-transparent or disclosed that they engaged in qualitatively worse practices of using personal information for third-party marketing purposes.

Therefore, parents, teachers, schools, and districts need to exercise caution when evaluating whether to use popular edtech applications, and vendors need to provide greater transparency on this issue, because a significant percentage of applications and services intended for children and students are using collected information for third-party marketing purposes without adequate notice and informed consent.

QUESTION: THIRD-PARTY MARKETING

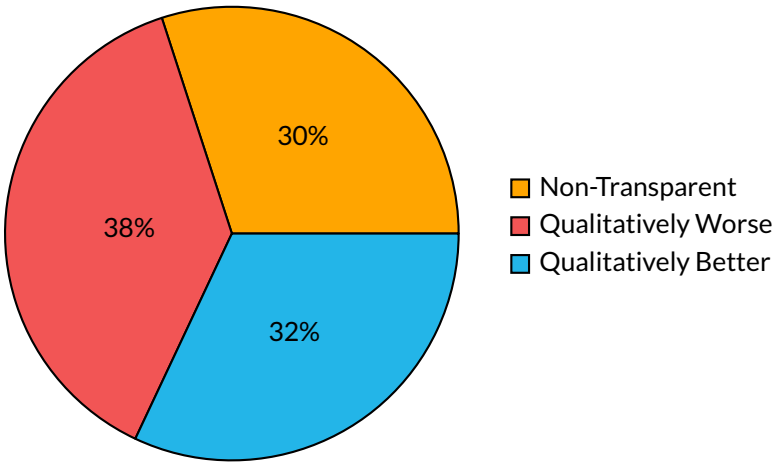


Figure 21: This chart illustrates the percentage of question responses for third-party marketing. Qualitatively better question responses indicate personal and nonpersonal information is never used for any third-party marketing purposes. Qualitatively worse question responses indicate personal and non-personal information may be used for third-party marketing purposes. Non-transparent responses indicate the terms are unclear about whether or not the application or service can use personal or non-personal information for any third-party marketing purposes.

42 *See supra* note 40.

43 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (an operator may display contextual advertisements to a child under the age of 13 without verifiable parental consent, under the "internal operations" exception).

44 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(b)(1)(A) (an operator is prohibited from using student data for targeted or behavioral advertising but not contextual advertising).

45 California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§22580-22582 (prohibits an operator from marketing or advertising non-age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile the personal information of a minor for the purpose of marketing or advertising non-age-appropriate types of products or services. Also, a minor is permitted to request to erase or remove and obtain removal of content or information posted on the operator's site).

Traditional Advertising

A majority of applications and services are non-transparent or explicitly allow traditional advertising. Among the applications and services we evaluated, approximately 17 percent disclosed a qualitatively better response that they do not display any traditional advertisements to children or students. In contrast, approximately 40 percent of applications and services disclosed they may display traditional advertisements to users as a means to monetize otherwise-free-to-use edtech tools. This evaluation question only examined whether or not the vendor discussed qualitatively better or worse practices for contextual advertising but not targeted, or behavioral, advertising.

Traditional advertisements (otherwise referred to as contextual advertisements) display products and services to users based only on the relevant content or webpage the user is currently viewing, but contextual ads do not collect any specific information about the user in order to display these ads beyond a user's search query or the webpage they visited. However, targeted advertisements do collect generalized information about users from various sources that include: demographic, location, gender, age, school, or interests. This information is collected in order to display products and services that may be more directed to users, to a more specific targeted audience, than simply contextual advertisements. Behavioral advertisements take targeted advertisements one step further and collect specific information about users typically through the use of cookies, beacons, tracking pixels, persistent identifiers, or other tracking technologies that provide more specific information about the user. This information is then shared with advertisers, who display even more targeted products and services than targeted advertisements to the user based on the information they received from the user's activities on the application or service. Parents and teachers assume that most free-to-use applications and services may display advertisements, and they often use these services with a lower expectation of privacy, but our analysis observed both free and paid services displaying advertisements. However, among the applications and services that required parent, teacher, or district paid subscriptions, or student in-app-purchases, the overwhelming majority did not display any form of advertising. Therefore, we observed a strong correlation of advertising use among the free applications and services evaluated, as compared to paid services. This likely results in an increased exposure to advertisements for children and students using only free versus paid applications and services, which can serve to normalize otherwise qualitatively worse advertising practices and lead to lower expectations of privacy for children and students.

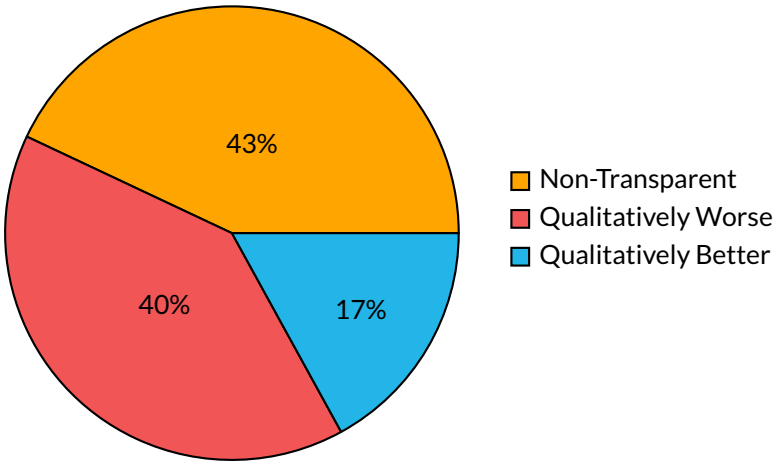
---

46 *See supra* note 43.

In contrast, approximately 43 percent of applications and services were non-transparent on this issue. Although observationally, we determined that, among applications and services that clearly displayed traditional advertisements, many did not disclose those practices in their policies. This behavior is likely because these applications and services believed the practice of displaying advertisements to be self-evident. Moreover, among applications and services that were non-transparent but did not display any advertisements, it is assumed their lack of transparency is because they do not believe they need to disclose otherwise qualitatively worse practices they do not engage in. However, when these practices are not transparently disclosed, there is no future expectation or trust on behalf of parents, teachers, schools, or districts about how information collected from children and students will be handled in order to meet their expectations of privacy.

Compared to our later analysis in the Behavioral Advertising section, more applications and services appeared to be non-transparent in their policies about contextual ads than in their policies about behavioral ads. Similarly, we observed a percentage increase in qualitatively better disclosures from vendors that do not display behavioral ads, but a decrease in the percentage of qualitatively worse practices relative to behavioral ads. Therefore, it appears applications and services are more likely to be non-transparent and disclose qualitatively worse practices about traditional ads rather than behavioral ads. However, this increase in the percentage of qualitatively worse disclosures is expected, as compliance obligations for applications and services intended for children provide an exception for vendors to display contextual advertising.[46] Lastly, the percentage increase of non-transparency on this issue as compared to that of behavioral advertising should also take into account potentially conflicting federal and state laws that provide an important distinction between contextual advertising directed at students.[47]

QUESTION: TRADITIONAL ADVERTISING



47 *See supra* note 44.

Figure 22: This chart illustrates the percentage of question responses about traditional advertising. Qualitatively better question responses indicate the application or service does not display any traditional advertisements to children and students. Qualitatively worse question responses indicate the application or service does display traditional advertisements to children and students. Non-transparent responses indicate the terms are unclear about whether or not the application or service displays traditional advertisements to children and students.

Behavioral Advertising

A roughly equivalent percentage of applications and services have either non-transparent, better, or worse practices regarding behavioral advertising. Among the applications and services we evaluated, approximately 32 percent disclosed a qualitatively better response that collected information is never used for any third-party behavioral advertising. In addition, approximately 5 percent disclosed not expected responses. From our previous analysis of personal information used for third-party marketing, we observed approximately the same 32 percent of applications or services disclosing that no collected information is used from children or students for advertising or marketing purposes. However, it appears that because the use of collected information for behavioral advertising poses a greater compliance risk from the perspective of vendors, we see a corresponding 11 percent decrease to only 29 percent disclosing qualitatively worse practices, as compared to the Third-Party Marketing section. In addition, we observed a similar increase of vendors remaining non-transparent on the issue, as compared to the Third-Party Marketing section. Accordingly, this shift to non-transparency from qualitatively worse disclosures on such an important compliance-related issue for children and students likely illustrates that many applications and services chose not to disclose substantive details about any behavioral advertising practices in order to avoid explicit disclosure of potential violations of federal or state law.[48, 49] It is also likely that among the applications and services that are non-transparent on this issue, many provide contextual advertising but do not feel comfortable explaining the compliance-related distinction between their use of contextual advertising but not behavioral advertising in context.[50]

---

48 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (an operator is prohibited from including behavioral advertisements or amassing a profile of a child under the age of 13 without parental consent).

49 *See supra* note 44.

50 *See supra* note 43.

Similarly with the Third-Party Marketing section, among the 39 percent of applications and services with qualitatively worse practices, many use language to restrict their use to only parent or teacher information for behavioral advertising purposes in order to avoid compliance issues with children or students. However, vendor compliance with this distinction is difficult, given that parents and teachers are not the primary users of these applications and services, but rather they are intended for children and students, who are generating the majority of behavioral data. From our evaluation process, we observed many applications and services that provide secondary "parent" or "teacher" accounts or related applications or services for monitoring of a child or student's progress through the primary data-collection product. Parents and teachers should exercise caution, because these accounts or services could potentially be used as a means to collect behavioral-related information from the parents and teacher themselves. This type of behavioral information could legally be used for advertising purposes and even directed back to the parents and teachers for educational-related products that could potentially be used directly, or indirectly, by their children or students.

QUESTION: BEHAVIORAL ADVERTISING

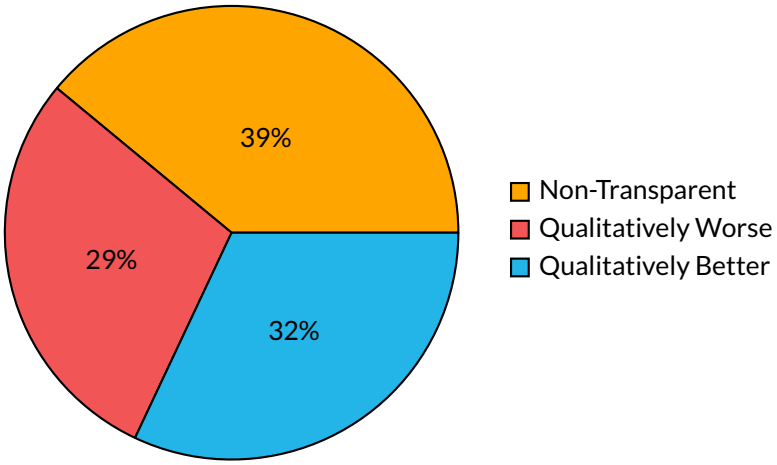


Figure 23: This chart illustrates the percentage of question responses about behavioral advertising. Qualitatively better question responses indicate the application or service does not display any behavioral advertisements to children and students. Qualitatively worse question responses indicate the application or service does display behavioral advertisements to children and students. Non-transparent responses indicate the terms are unclear about whether or not the application or service displays behavioral advertisements to children and students.

Third-Party Tracking

A majority of applications and services are non-transparent or explicitly allow third-party tracking. Among the applications and services we evaluated, approximately 21 percent disclosed a qualitatively better response that collected information will never be used by third-party advertising or tracking technologies. Accordingly, collection of information from children or students using persistent identifiers or third-party scripts that can be used to recognize and track users is considered qualitatively worse in our evaluation process, because tracking in this manner can be used for exfiltration of sensitive data through unknown processes or for marketing or advertising purposes.[51, 52] From our analysis, it appears there is an approximately 11 percent lower occurrence in the disclosure of qualitatively better practices for this issue, as compared to the Behavioral Advertising section, but a relative increase in qualitatively worse practices to approximately 37 percent. Furthermore, it appears that most applications and services evaluated are non-transparent about whether or not they use third-party advertisement trackers. This shift to non-transparency and qualitatively worse practices of marketing-related practices is non-conforming but also unsurprising given the recent explosion of desktop and mobile third-party advertising trackers used in mainstream web applications and services in only the past few years.[53, 54] Therefore, we would expect more policies to include transparent qualitative responses on this issue year over year as it becomes an increasingly important privacy expectation for parents and teachers and an important differentiating feature when choosing between competing educational applications and services.

In addition, our evaluation process observationally determined that the majority of services evaluated do not provide third-party advertising trackers on their websites. However, we did not observationally evaluate third-party advertising trackers used with mobile applications. The lack of third-party advertising trackers is expected in this context, given that these are popular educational services and vendors ostensibly wish to avoid similar compliance issues of collecting behavioral information from children and students. However, unlike other marketing or advertising indicators, it appears vendors are neither aware, nor believe, there is currently a comparative advantage to disclosing

---

51 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (an operator is prohibited from sharing a persistent identifier collected from children that can be used to recognize and track a user over time and across different websites or services without verifiable parental consent).

52 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(7) (an operator may provide a hyperlink in their privacy policy to a location containing a description, including the effects, of any program or protocol that offers the consumer a choice not to be tracked).

they do not engage in the qualitatively worse practice of third-party tracking. Given that approximately 42 percent of applications and services are non-transparent on this issue, it is recommended that vendors change their disclosure practices in order to provide more notice to consumers about whether or not their product uses third-party advertising trackers; third-party tracking practices are ultimately no different from other methods of collecting behavioral information for marketing or advertising purposes.

QUESTION: THIRD-PARTY TRACKING

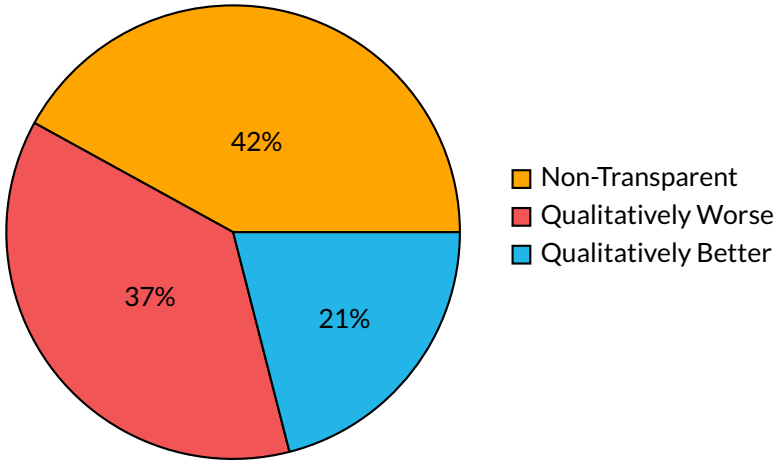


Figure 24: This chart illustrates the percentage of question responses about third-party tracking. Qualitatively better question responses indicate collected information will never be used by third-party advertising or tracking technologies. Qualitatively worse question responses indicate collected information may be used by third-party advertising or tracking technologies. Non-transparent responses indicate the terms are unclear about whether or not collected information can be used by third-party advertising or tracking technologies.

53 Lerner, Adam & Simpson, Anna Kornfeld, et al., *Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016* (2016), https://trackingexcavator.cs.washington.edu/InternetJonesAndTheRaidersOfTheLostTrackers.pdf.

54 Razaghpanah, Abbas & Nithyanand, Rishab, et al., *Apps, Trackers, Privacy, and Regulators, A Global Study of the Mobile Tracking Ecosystem* (2018), https://www.ndss-symposium.org/wp-content/uploads/sites/25/2018/02/ndss2018_05B-3_Razaghpanah_paper.pdf.

Track Users

A majority of applications and services are non-transparent or explicitly track users across other websites. Among the applications and services we evaluated, approximately 28 percent disclosed a qualitatively better response that collected information will never be used to track and target advertisements to users on other third-party websites or services. Similarly to the Third-Party Tracking section, collection of information from children or students using persistent identifiers or third-party scripts that can be used to recognize and track a user across other websites is considered qualitatively worse in our evaluation process, because tracking users in this manner can be used for exfiltration of sensitive data through unknown processes or for marketing or advertising purposes.

From our analysis, it appears there is an approximately 16 percent lower occurrence of qualitatively worse practices, as compared to the Third-Party Tracking section. This decrease is significant, because it highlights an important distinction that vendor's policies make between engaging directly or indirectly in advertising tracking practices: direct (by placing those tracking technologies on their service) or indirect (by providing third parties with persistent identifier information from users) for third-party marketing or advertising purposes on other services. Similarly to the Third-Party Marketing section, among the 21 percent of applications and services with qualitatively worse practices, a majority of policies use language to try to restrict their use of tracking to only parent or teacher information in order to avoid compliance issues with children or students. However, this distinction is difficult to apply in practice and may not adequately exculpate vendors from potential compliance violations of tracking children or students.[55, 56, 57, 58] From our analysis, it appears vendors are not predisposed to disclose whether third parties may collect personal information about children's or students' online activities over time and across different websites, as required by state law.[59] Moreover, the relative percent increase in non-transparency and qualitatively better practices, as compared to the Third-Party Tracking section, is likely the result of both vendors remaining unaware of the difference between first- and third-party tracking and vendors choosing to carefully differentiate the qualitatively better practice of not sharing collected persistent identifiers that they may use themselves with other third parties for their own advertising or marketing purposes.

QUESTION: TRACK USERS

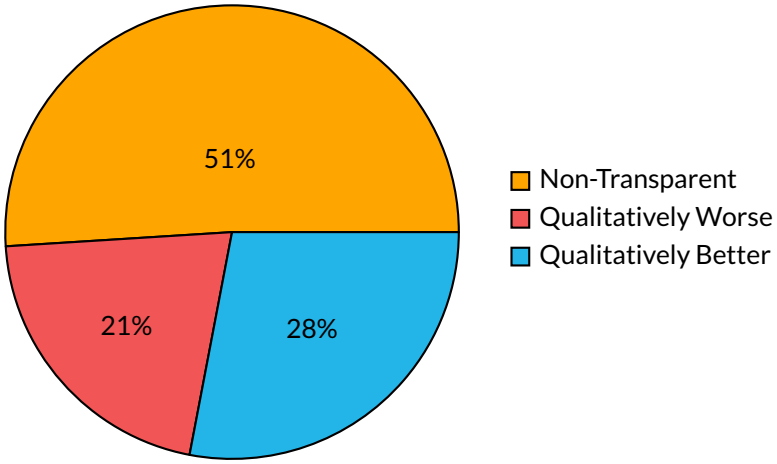


Figure 25: This chart illustrates the percentage of question responses about tracking users. Qualitatively better question responses indicate collected information will never be used to track and target advertisements to users on other third-party websites or services. Qualitatively worse question responses indicate collected information may be used to track and target advertisements to users on other third-party websites or services. Non-transparent responses indicate the terms are unclear about whether or not collected information can be used to track and target advertisements to users on other third-party websites or services.

Ad Profile

A majority of applications and services are non-transparent about creating advertising profiles. Among the applications and services we evaluated, approximately 26 percent disclosed a qualitatively better response that collected information will never be used by the vendor to create an advertising profile, engage in data enhancement, or target advertising. Accordingly, collection of information from children or students to amass an advertising profile or share that information with third parties for data enhancement is considered qualitatively worse in our evaluation process, because it is

55 *See supra* note 51.

56 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1 ("personal information" under FERPA includes direct identifiers such as a student or family member's name, or indirect identifiers such as date of birth or mother's maiden name, or other information that is linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty).

57 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(b)(1)(B) (an operator is prohibited from tracking a student across websites with targeted advertising).

58 *See supra* note 45.

59 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(6) (an operator is required to disclose whether other third parties may collect personally identifiable information about a consumer's online activities over time and across different websites).

considered another indirect method by which to share information for marketing, advertising, or automated decision-making purposes. Profiling in our evaluation process means the automated processing of personal data to evaluate certain personal aspects relating to a specific child or student, in order to analyze or predict aspects concerning that child or student for marketing or advertising purposes.[60, 61, 62, 63, 64] As compared with other marketing or advertising indicators in our evaluation, this issue has the highest relative percentage of non-transparency and lowest percentage of qualitatively worse disclosures. Simply stated: The majority of applications and services evaluated are not even aware of this issue. Among the approximately 64 percent that were non-transparent, it appeared vendors did not understand the distinction between using personal information for advertising or marketing purposes and using non-personal information for amassing a profile or sharing that generated profile information with third parties for subsequent data combination or enhancement. In practice, applications and services can place contractual limitations on third parties in which they share data that describe how personal and non-personal information can be used. Accordingly, approximately 70 percent of applications and services disclosed qualitatively better practices, that they place contractual limitations on third parties, which can mitigate otherwise non-transparent responses to whether collected information can be used to create an advertising profile.[65, 66, 67, 68]

The existence of automated decision-making, including profiling children or students for advertising purposes, is likely misunderstood by vendors as behavioral advertising or third-party tracking. However, vendors should be aware that amassing and using a broader profile of a child or student for non-K–12 educational purposes is a violation of use of collected information, because the amount and type of collected data goes beyond the scope of behavioral information, and the prohibition on use goes beyond simply advertising or marketing purposes. Therefore, parents and teachers need to

---

60 *See supra* note 48.

61 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(b)(2) (an operator is prohibited from amassing a profile of a student).

62 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(e)(2) (an operator may share student data with third parties for legitimate research purposes if it is not used for advertising or to amass a profile on a student for purposes other than K–12 school purposes).

63 *See supra* note 45.

64 *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(4); General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art. 13(2)(f); General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(g); General Data Protection Regulation (GDPR), Right of access by the data subject, Art. 15(1)(h); General Data Protection Regulation (GDPR), Automated individual decision-making, including profiling, 22(1)–(3).

exercise caution with advertising profiles when evaluating whether to use popular edtech applications and services, and vendors need to provide greater transparency on this issue. When these practices are not transparently disclosed, there is no future expectation or trust on behalf of parents, teachers, schools, or districts about how collected information from children and students will be handled in order to meet their expectations of privacy.

QUESTION: AD PROFILE

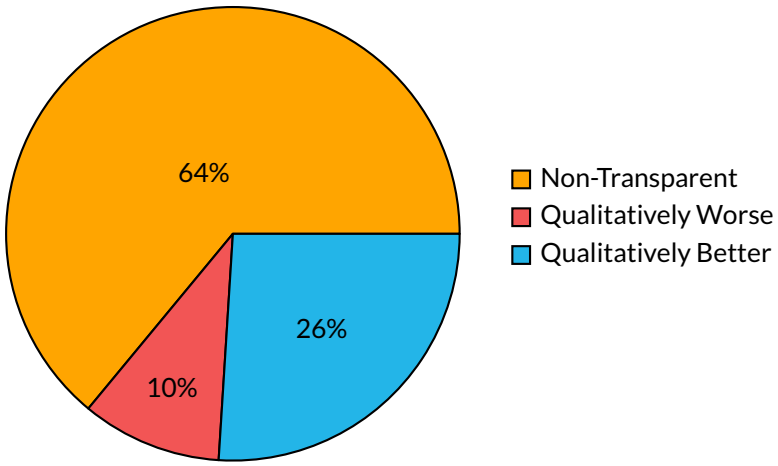


Figure 26: This chart illustrates the percentage of question responses about ad profiling. Qualitatively better question responses indicate third parties cannot create an advertising profile, engage in data enhancement, or target advertising. Qualitatively worse question responses indicate third parties can create an advertising profile, engage in data enhancement, or target advertising. Non-transparent responses indicate the terms are unclear about whether or not third parties can create an advertising profile, engage in data enhancement, or target advertising.

65 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8 (an operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information and provide assurances that they contractually maintain the information in the same manner).

66 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(b)(4)(E)(i) (an operator may disclose student information to a third-party service provider, but the third party is prohibited from using the information for any purpose other than providing the service).

67 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(b)(4)(E)(ii) (a third-party service provider may not disclose student information to any subsequent third party).

68 *See* General Data Protection Regulation (GDPR), Processor, Art. 28(2)–(4); General Data Protection Regulation (GDPR), Processing under the authority of the controller or processor, Art. 29.

Transfer of Data

A majority of applications and services are non-transparent or explicitly allow the onward transfer of data. Among the applications and services we evaluated, approximately 74 percent disclosed a qualitatively worse response that collected information can be transferred to a successor third party in the event of a merger, acquisition, or bankruptcy. Accordingly, transferring collected information to a third-party successor as an asset is considered qualitatively worse in our evaluation process, because transferred data can include personal and non-personal information that was collected for the specific purpose of using the application and service and not for any other purpose that includes monetization through a third-party transfer. Transferring users' information collected from the application or service to a third party can change the context in which the data is used or disclosed by that third party with unintended consequences. This raises additional questions about whether personal information that is not required to use the application or service should be collected or aggregated in the first place; this creates an incentive to use collected information as an asset to be transferred to third parties. This practice can be mitigated, however, as illustrated in our analysis in the Collection Limitation section, where approximately 58 percent of applications and services disclosed that they limit the collection of information. Limiting the collection of information in this manner can change the incentive model to transfer information as an asset, because there would be less information available to transfer to third parties.

However, approximately 23 percent of applications and services are non-transparent about whether collected information can be transferred to a successor third party in the event of a merger, acquisition, or bankruptcy. Lack of transparency on this issue means applications and services still reserve the right to transfer collected information to third parties, if not otherwise prohibited by private contractual agreements. Therefore, a majority of approximately 97 percent of applications and services may transfer collected information in this context, and in many cases they may transfer information without contractual limitations or obligations on the third-party recipient.[69] Many applications and services are non-transparent about whether or not the third-party successor of a data transfer is contractually required to provide the same level of privacy protections as the vendor. However, even with contractual obligations in place, most applications and services do not provide users the ability to opt out of a data transfer to a third party. Therefore, third parties can still use and disclose transferred information in an anonymous or de-identified format or use information in a different context. Context matters when transferring data because policies often do not require consent from users to use collected information in a context different from that in which it was collected.

QUESTION: TRANSFER DATA

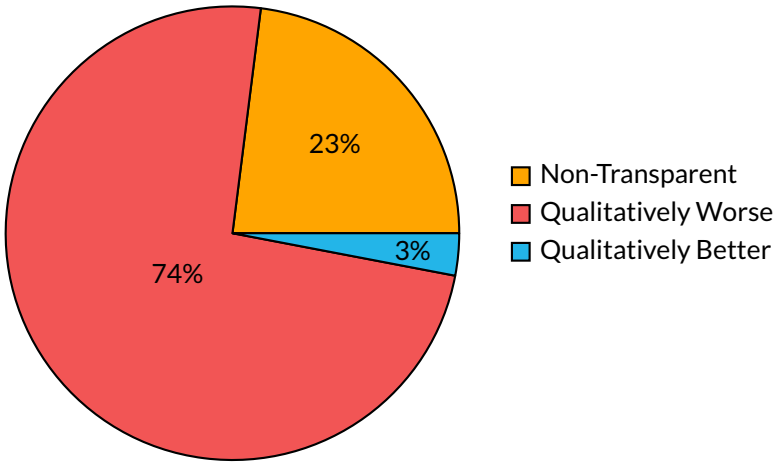


Figure 27: This chart illustrates the percentage of question responses about transferring data. Qualitatively better question responses indicate the application or service does not transfer collected information to a successor third party in the event of a merger, acquisition, or bankruptcy. Qualitatively worse question responses indicate the application or service may transfer collected information to a successor third party in the event of a merger, acquisition, or bankruptcy. Non-transparent responses indicate the terms are unclear about whether or not the application or service may transfer collected information.

69 *See supra* note 40.

CONCERNS

The privacy-evaluation process also translates the policies of an application or service into four concerns that can be used to quickly identify and describe the safety, privacy, security, or compliance practices of a vendor's policies. These four concerns are mapped to specifically related evaluation questions that provide each concern with its own transparency, quality, and overall score relative to that concern.[70] For example, the percentage of questions answered for a particular concern indicates its transparency score, and percentage of relative better or worse responses to questions for that concern also indicate its quality score. The scoring methodology for the concerns is the same as the methodology used for the Statute Scoring section as opposed to the overall scoring. That is, each question in a particular concern is scored as though it is expected to be answered. Table 5 below summarizes our findings of the minimum, mean, lower-quartile (Q1), median (Q2), upper-quartile (Q3), maximum, and standard deviation for each concern's transparency, quality, and overall score.

CONCERN SCORING SUMMARY STATISTICS

Score Type	Min.	Mean	$Q1$	Median($Q2$)	$Q3$	Max.	Stdev
Safety Transparency	0	31	10	30	47	100	24
Safety Quality	0	25	0	24	33	100	23
Safety Overall	0	14	2	11	21	80	15
Privacy Transparency	22	66	59	68	79	93	16
Privacy Quality	44	68	57	68	78	100	13
Privacy Overall	16	48	41	47	55	74	12
Security Transparency	39	66	54	63	76	95	14
Security Quality	0	73	68	75	86	100	20
Security Overall	6	52	40	52	64	88	18
Compliance Transparency	0	51	37	52	70	96	23
Compliance Quality	0	60	50	68	77	88	24
Compliance Overall	0	38	21	39	56	76	21

Table 5: This table illustrates summary statistics for transparency, quality, and overall score for each concern.

From the table it is apparent the concerns for privacy and security both have similar means for transparency, quality, and overall score, but as our later analysis will demonstrate, their frequency distribution range of scores is quite different. Also, the mean

70 Common Sense Media, *Privacy Questions, Organized by Concern*, https://www.commonsense.org/education/privacy/questions/concerns.

for safety transparency is higher than the mean for safety quality, which illustrates the relationship between transparency and qualitatively worse disclosures for safety issues. In contrast, the mean for compliance transparency is lower than the mean for compliance quality, indicating that when applications or services are transparent about compliance obligations, they are more likely to disclose qualitatively better practices.

Within each of the four concerns of safety, privacy, security, and compliance are five primary evaluation questions that are strong indicators for understanding the context of what issues are most illustrative for each particular concern. These primary concern evaluation questions are strong overall indicators for all of a particular concern's scores, because they are typically weighted more heavily than other evaluation questions within that concern based on several factors and therefore contribute more to that particular concern's transparency, quality, and overall score. These five primary indicators help provide more context about the different issues that make up a particular concern for an application or service and ultimately provide parents and teachers with more relevant information with which to make a better informed decision about whether to use a particular application or service based on the concerns that matter most.

Safety Indicators

Among the applications or services we evaluated, the concern of safety primarily examines practices wherein children's or students' information could be made publicly visible to others and wherein social interactions with other children or strangers are made available.

Safety Transparency

Figure 28 illustrates the frequency of safety transparency scores among all applications and services evaluated. From the analysis, we determined a mean of approximately 31/100. This mean is lower than one would expect, given that the services evaluated are intended for children and students. However, the safety concern consists of only 16 related questions, and therefore the lower mean result is likely attributable to two factors: First, most applications and services do not include in their products safety-related features that would allow children or students to make personal or non-personal information visible or provide any social interactions with others. These services are not likely to disclose information about safety features or controls they do not otherwise provide. Second, applications and services are likely not aware they should

provide notice in their policies about common safety risks, such as children or students making personal information visible, or the possibility of social interactions with strangers. Transparently providing not-expected-to-be-disclosed information about common safety features for applications and services that are intended for children and students is a qualitatively better practice, because it provides parents, teachers, and schools with more information to make an informed decision about the safety of that product in their context. As a result, Figure 28 displays skewed transparency scores where approximately 20 percent of applications and services evaluated were completely non-transparent on all safety-concern-related questions.

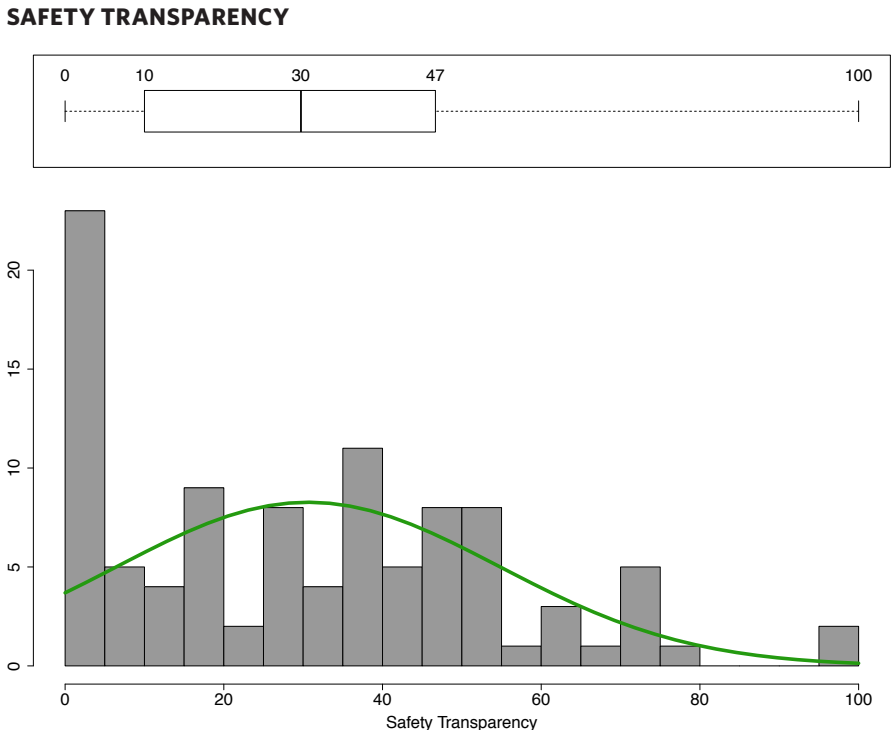


Figure 28: This chart illustrates the safety transparency score distribution histogram and normal curve with median (Q2) 30, lower quartile (Q1) 10, upper quartile (Q3) 47, lower whisker 0 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 100 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Safety Quality

Figure 29 illustrates the frequency of safety quality scores among all applications and services evaluated. From the analysis, we determined a mean of approximately 25/100. Similarly to the Safety Transparency section, this mean is skewed and lower than one would expect, given that the services evaluated are intended for children and students. However, this is likely attributable to the fact that most applications and services that

are transparent about safety also disclosed qualitatively worse safety practices. These responses are more likely to be qualitatively worse, because features relating to visibility of information and communications with others inherently place children's and students' information more at risk. There is an increased risk for the safety of children and students with these practices, because their information could be made publicly visible to others or could be shared through social interactions with strangers.

The evaluation process does not make a quantitative differentiation in quality scores between applications or services that may place restrictions or controls on their safety features and those that may not. For example, parent or teacher restrictions on which data can be made available, and restrictions on which individuals a child or student can communicate with, are not reflected in the safety quality score. Therefore, our strict evaluation process indicates that applications or services that simply provide any of these features would receive a lower quality score, with the expectation that parents, teachers, schools, and districts should learn more about the safety protections or controls in place to help mitigate these risks.

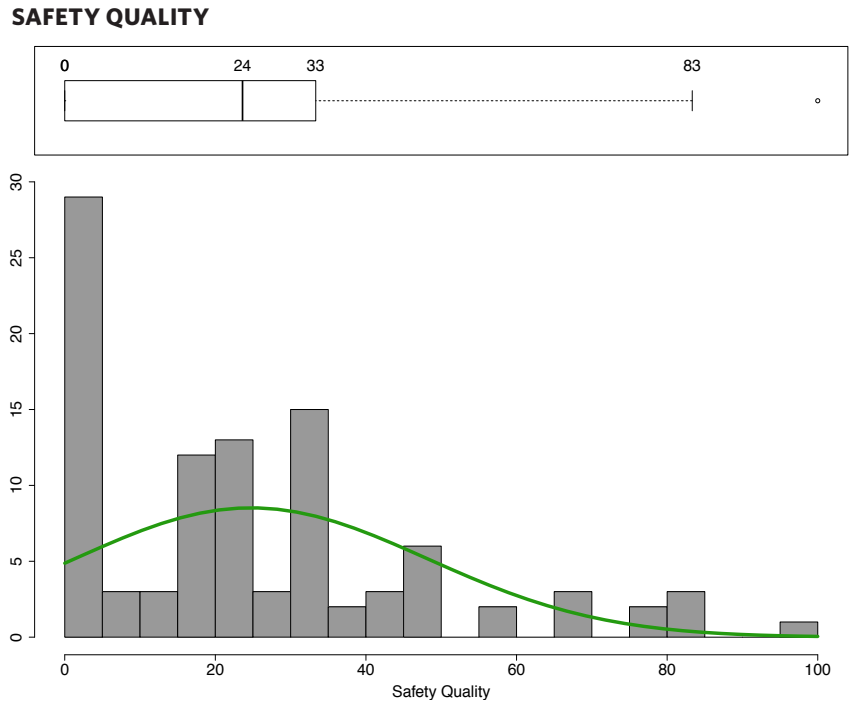


Figure 29: This chart illustrates the safety quality score distribution histogram and normal curve with median (Q2) 24, lower quartile (Q1) 0, upper quartile (Q3) 33, lower whisker 0 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 83 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Safety Overall Score

Figure 30 illustrates the frequency of safety overall scores among all applications and services evaluated for the concern of safety. From the analysis, we determined a mean of approximately 14/100. Similarly to the Safety Transparency and Safety Quality sections, this mean is skewed and lower than expected, given the services evaluated are intended for children and students. The lower-than-expected mean is likely attributable to applications and services choosing to be non-transparent about disclosing safety practices they do not provide. However, if applications and services do provide features such as social interactions, their disclosures are more likely to be qualitatively worse. Therefore, parents and teachers would likely benefit from more transparency of safety-related information about applications and services such as: whether children's or students' information can be made publicly visible to others, or whether social interactions with other children, students, or strangers are available. These features are important differentiating factors for parents, teachers, schools, and districts when choosing among applications or services, and vendors are recommended to increase their transparency on these important safety issues.

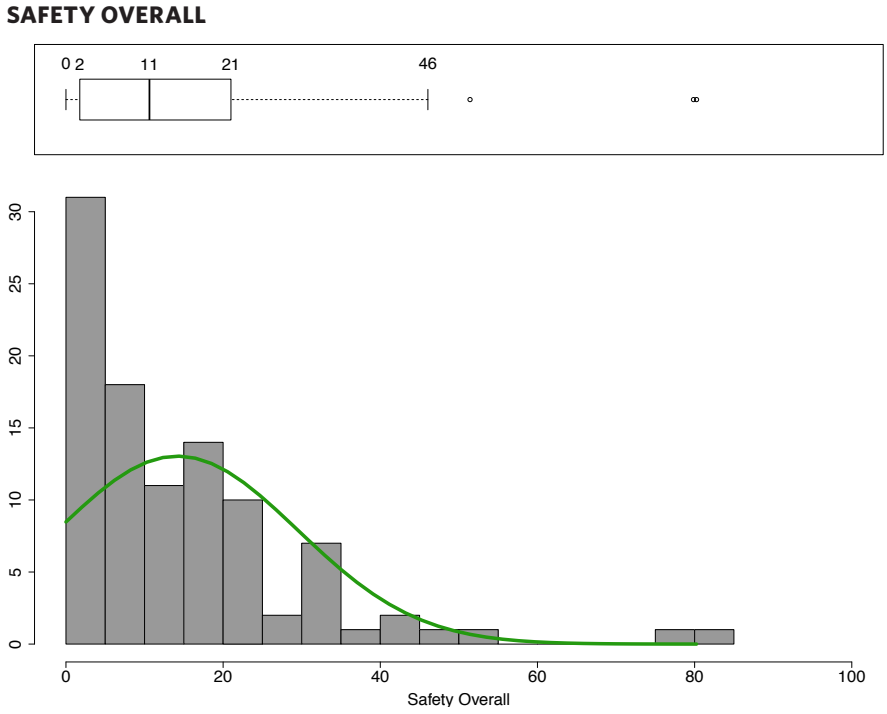


Figure 30: This chart illustrates the safety overall score distribution histogram and normal curve with median (Q2) 11, lower quartile (Q1) 2, upper quartile (Q3) 21, lower whisker 0 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 46 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Unsafe Interactions

Among the applications or services we evaluated, approximately 12 percent disclosed that if social interactions are available, those interactions are only available with other children or that students can interact only with other students or teachers in the same classroom or school. This finding is lower than expected, likely because most applications or services evaluated are non-transparent about whether or not they provide safe interaction features. However, this unexpectedly low qualitatively better percentage may be attributable to mitigating issues discussed in the Moderate Interactions section below. Furthermore, we assume among the approximately 54 percent of non-transparent responses to this question that otherwise provide safe interactions, there likely is a statistically significant percentage that have qualitatively better practices but did not disclose whether those restrictions or controls are in place by default. In contrast, approximately 34 percent of applications and services disclosed that social interactions could occur between children or students with strangers or adults, practices that may be in violation of federal law if appropriate protections are not put in place.[71] From our analysis, we observed applications and services that provided unmoderated chat rooms, forums, open text fields, and comment areas. These features were typically provided to children and students without sufficient safety protections in place. Therefore, it is recommended that vendors increase their transparency on this important safety issue and put stronger safety protections and controls in place by default to help parents, teachers, schools, and districts learn more about the safety features in place to help mitigate these risks.

71 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (an operator is prohibited from making personal information from a child publicly available in an identifiable form by any means, including a public posting through the internet or through a personal home page or screen posted on a website or online service, a pen pal service, an electronic mail service, a message board, or a chat room).

SAFETY: UNSAFE INTERACTIONS

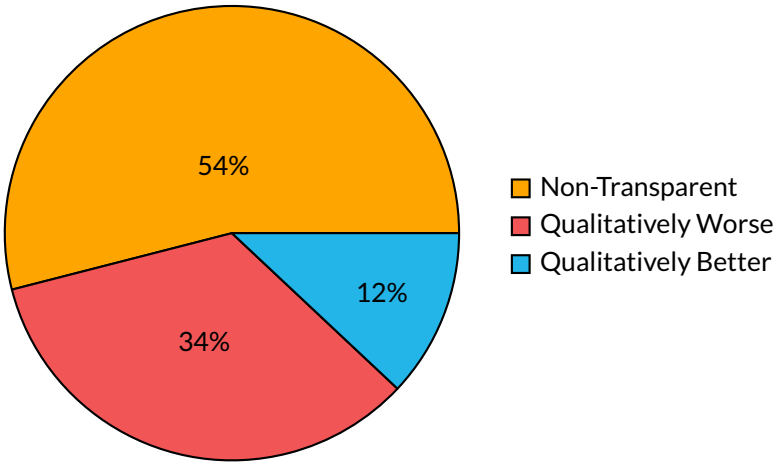


Figure 31: This chart illustrates the percentage of question responses about unsafe interactions. Qualitatively better question responses indicate social interactions are only available with other children or that students can interact only with other students or teachers in the same classroom or school. Qualitatively worse question responses indicate social interactions may be available between strangers or adults. Non-transparent responses indicate the terms are unclear about whether or not social interactions are only available with other children or that students can interact only with other students or teachers in the same classroom or school.

Moderate Interactions

Among the applications or services we evaluated, approximately 11 percent disclosed a qualitatively better response that interactions between users of the application or service are moderated. This disclosure is significantly lower than expected, given that the practice of moderating social interactions mitigates the otherwise 34 percent of applications and services as described in unsafe interactions that disclosed qualitatively worse practices of not providing safe social interactions with children or students. Accordingly, the approximately 13 percent that disclosed qualitatively worse responses that they do not moderate social interactions between users also disclosed that those services are not intended for children or students. However, 76 percent of applications and services evaluated were non-transparent on this question, likely because they do not provide social-interaction features, or, if these features are available, it is not evident to vendors that this compliance obligation should be disclosed in their policies.

It is recommended that applications and services that provide social interactions for children and students under 13 years of age disclose in their policies that they are in

compliance with federal law by moderating interactions or postings before they are made publicly available to others.[72, 73]

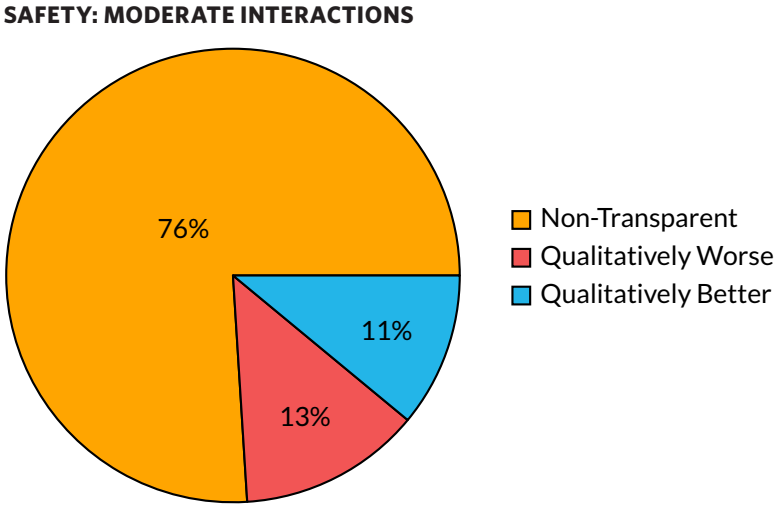


Figure 32: This chart illustrates the percentage of question responses about moderate interactions. Qualitatively better question responses indicate social interactions between users are moderated. Qualitatively worse question responses indicate social interactions between users are not moderated. Non-transparent responses indicate the terms are unclear about whether or not social interactions between users are moderated.

Visible Data

Among the applications or services we evaluated, approximately 15 percent disclosed a qualitatively better response that no personal information can be displayed publicly. Similarly to the Unsafe Interactions section, this finding is not surprising, as most applications or services evaluated are non-transparent about this issue. In addition, approximately 10 percent disclosed not-expected responses. The approximately 35 percent of non-transparent responses to this question likely have a significant percentage that have otherwise qualitatively better practices but do not disclose what those practices are. However, approximately 50 percent of applications and services disclosed qualitatively worse practices whereby children's or student's information could be made publicly visible. Parents and teachers need to exercise caution when evaluating whether to use popular edtech applications, and vendors need to provide greater transparency on

72 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (an operator may prevent collection of personal information if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete the information from its records).

73 *See supra* note 71.

this issue, because these findings suggest most applications or services intended for children or students have possible compliance violations in regards to making personal information publicly visible online.[74, 75]

SAFETY: VISIBLE DATA

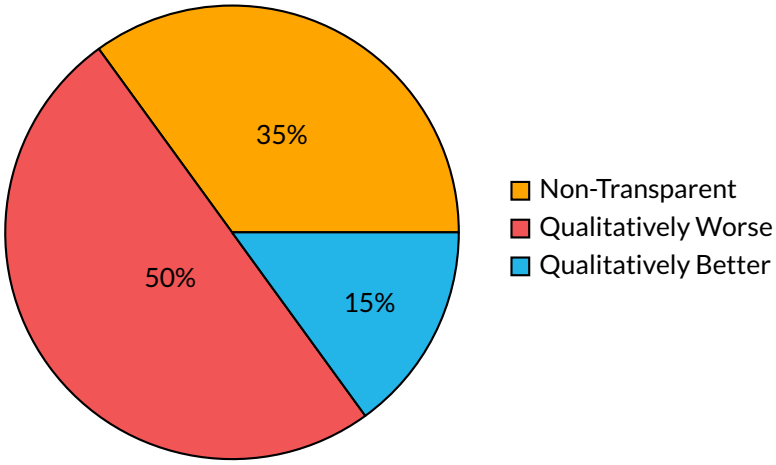


Figure 33: This chart illustrates the percentage of question responses about visible data. Qualitatively better question responses indicate personal information cannot be displayed publicly. Qualitatively worse question responses indicate personal information can be displayed publicly. Non-transparent responses indicate the terms are unclear about whether or not personal information can be displayed publicly.

Monitor Content

Among the applications or services we evaluated, only approximately 14 percent disclosed a qualitatively better response that user-uploaded content is reviewed, screened, or monitored by the vendor. Accordingly, this practice is qualitatively better because these applications and services are intended for children and students, and the practice of monitoring content includes removing non-age-appropriate references to such things as alcohol, gambling, violence, or sex. The majority of applications and services evaluated do not provide features for users to upload or create photographic or video content but rather limit media consumption to the content provided by the service or to user-created text-based comments. Therefore, our finding that indicate approximately 61 percent are non-transparent on this question is not surprising.

74 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(2) (an operator is required to disclose whether the service enables a child to make personal information publicly available).

75 *See supra* note 71.

However, approximately 25 percent of applications or services disclosed they provide users the ability to upload and share content with others but put no automatic or manual protections in place to review, screen, or monitor user-generated content. Not monitoring any user-generated content is considered a qualitatively worse practice in our evaluation process, because not implementing technological screening protections may expose children and students to obscene or offensive content. If vendors do not have manual or automatic screening protections in place, children or students may be exposed to non-age-appropriate content that may be harmful, and the only recourse from parents and teachers is to request removal of harmful content after it has been viewed. Moreover, schools and districts may have E-rate-related compliance obligations to monitor user content if these applications or services are used with students.[76]

SAFETY: MONITOR CONTENT

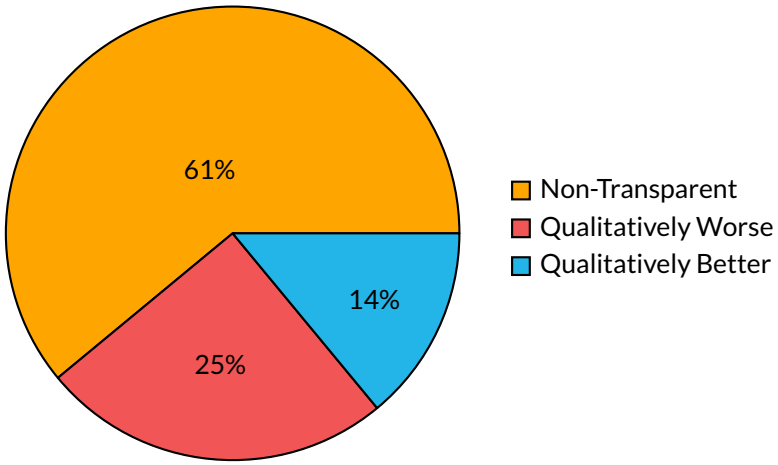


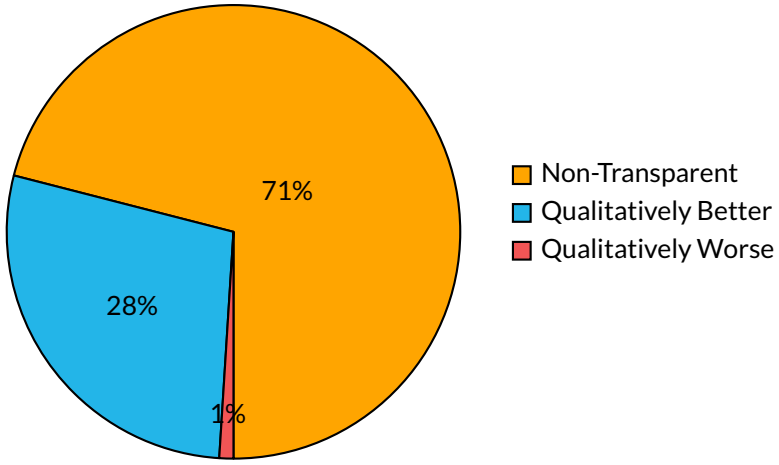
Figure 34: This chart illustrates the percentage of question responses about monitoring content. Qualitatively better question responses indicate user content is reviewed, screened, or monitored by the vendor. Qualitatively worse question responses indicate user content is not reviewed, screened, or monitored by the vendor. Non-transparent responses indicate the terms are unclear about whether or not user content is reviewed, screened, or monitored by the vendor.

76 Children's Internet Protection Act (CIPA), 47 U.S.C. §254(h)(5)(B) (a K–12 school under E-rate discounts is required to adopt a policy of internet safety for minors that includes monitoring the online activities of minors and the operation of a technology-protection measure with respect to any of its computers with internet access that protects against access to visual depictions that are obscene, child pornography, or harmful to minors).

Safe Tools

Among the applications or services we evaluated, approximately 28 percent disclosed a qualitatively better response that tools and processes that support safe and appropriate social interactions or digital citizenship are disclosed in the policies. Given that the applications and services evaluated are intended for children and students, this question provides greater insight into whether additional information is made available for parents and teachers to learn about the safety issues and tools available for children and students to make safe, smart, and ethical decisions online and avoid content that may be harmful.[77, 78, 79, 80] From our analysis, the approximately 16 percent, 17 percent, and 14 percent relative increase in qualitatively better responses compared to those in the Unsafe Interactions, Moderate Interactions, and Monitoring Content sections respectively is likely attributable to applications and services that do not provide social interactions or creation of user content but otherwise still provide additional resources to help parents and teachers learn more about keeping children and students safe online. However, approximately 71 percent of applications and services evaluated were non-transparent and did not disclose any resources in their policies to help parents or teachers learn about how to keep children and students safe online while using their products.

SAFETY: SAFE TOOLS



77 *Id.*

78 *See supra* note 45.

79 The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(d) (a provider of an interactive computer service shall notify the customer that parental-control protections [such as computer hardware, software, or filtering services] are commercially available and may assist the customer in limiting access to material that is harmful to minors).

80 Common Sense Media, *Digital Citizenship*, https://www.commonsense.org/education/digital-citizenship.

Figure 35: This chart illustrates the percentage of question responses about safe tools. Qualitatively better question responses indicate that tools and processes that support safe and appropriate social interactions or digital citizenship are disclosed. Qualitatively worse question responses indicate that tools and processes that support safe and appropriate social interactions or digital citizenship are not disclosed. Non-transparent responses indicate the terms are unclear about whether or not tools and processes that support safe and appropriate social interactions or digital citizenship are disclosed.

Privacy Indicators

Among the applications or services we evaluated, the concern of privacy primarily examines practices wherein children's or students' information is collected, used, and shared with third parties and any limitations placed on those practices.

Privacy Transparency

Figure 36 illustrates the frequency of privacy transparency scores among all applications and services evaluated for the concern of privacy. From the analysis, we determined a mean of approximately 66/100. This mean is lower than expected, given these applications and services are intended for children and students and therefore expected to provide more child and student privacy-related disclosures. However, this wide distribution range of privacy transparency scores from 83 privacy concern questions illustrates that vendors are likely predisposed to non-transparency of privacy-related issues in their policies. From our analysis, we observed that the behavior of non-transparency is commonplace among all the privacy-evaluation questions, because it serves to minimize potential liability for vendors in disclosing qualitatively worse practices or making promises in their policies they are otherwise unable to keep.

PRIVACY TRANSPARENCY

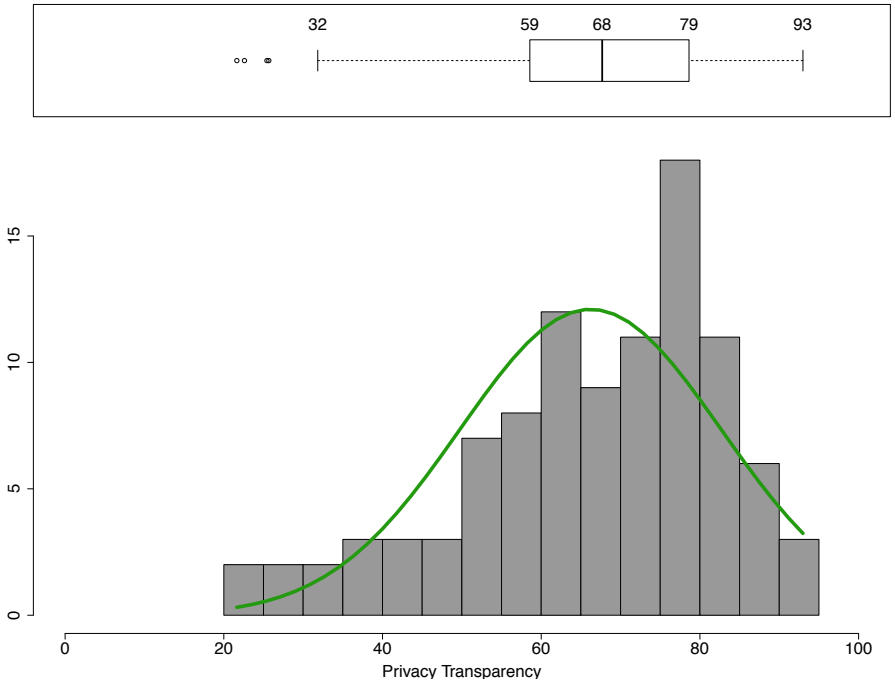


Figure 36: This chart illustrates the privacy transparency score distribution histogram and normal curve with median (Q2) 68, lower quartile (Q1) 59, upper quartile (Q3) 79, lower whisker 32 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 93 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Privacy Quality

Figure 37 illustrates the frequency of privacy quality scores among all applications and services evaluated for the concern of privacy. From our analysis, we determined a mean of approximately 68/100. Similarly to privacy transparency, this mean is lower than expected, given that the applications and services evaluated are intended for children and students. However, the high concentration of privacy quality scores above 45 indicates most applications and services that are transparent about privacy also disclose qualitatively better practices. This concentration of quality scores also illustrates that most privacy-related qualitative statements made in policies are more homogeneous than other concerns.

PRIVACY QUALITY

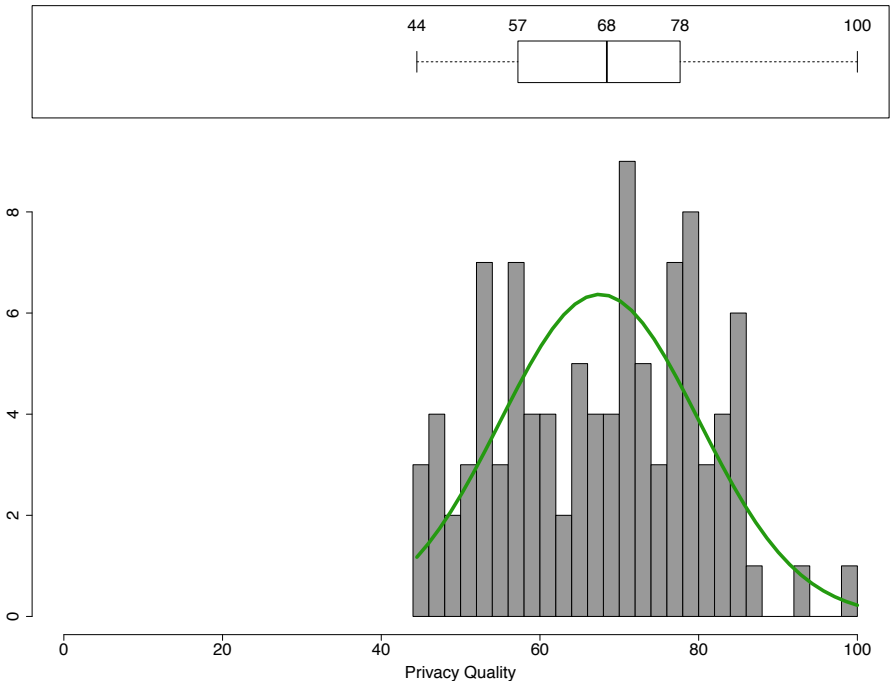


Figure 37: This chart illustrates the privacy quality score distribution histogram and normal curve with median (Q2) 68, lower quartile (Q1) 57, upper quartile (Q3) 78, lower whisker 44 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 100 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Privacy Overall Score

Figure 38 illustrates the frequency of privacy overall scores among all applications and services evaluated for the concern of privacy. From the analysis, we determined a mean of approximately 48/100. Similarly to the Privacy Transparency and Privacy Quality sections, this mean is lower than expected, given the applications and services evaluated are intended for children and students. As discussed, this lower-than-expected mean for the privacy overall score is likely a result of applications and services remaining non-transparent about disclosing expected privacy practices they may or may not provide.

PRIVACY OVERALL

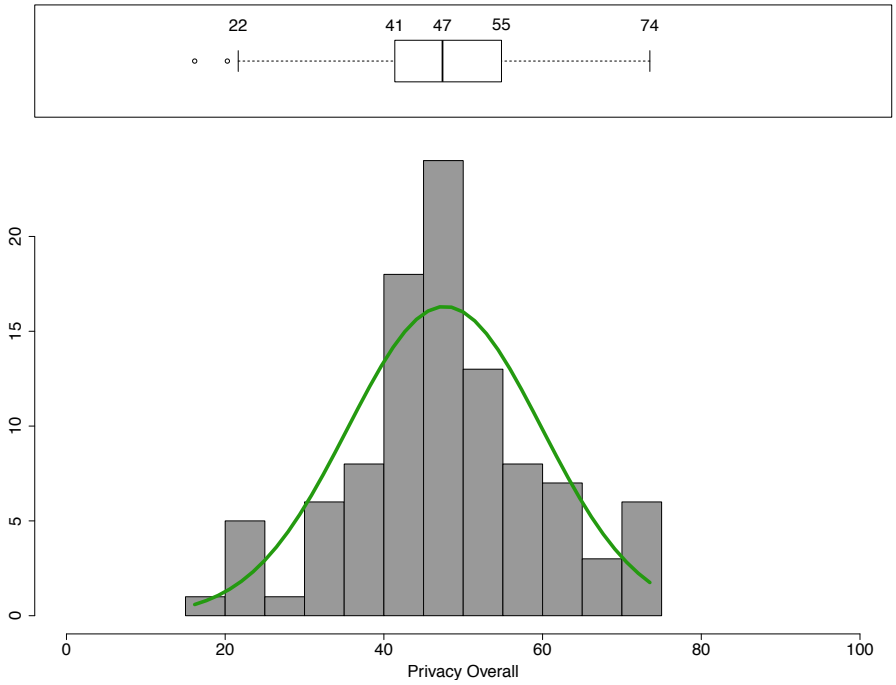


Figure 38: This chart illustrates the privacy overall score distribution histogram and normal curve with median (Q2) 47, lower quartile (Q1) 41, upper quartile (Q3) 55, lower whisker 22 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 74 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Moreover, the privacy overall score is unique in that there is a strong linear correlation between the privacy overall score and an application or services' otherwise overall score. This is expected given that the subset of privacy-related questions used for the privacy concern are a disproportionate number of the overall number of evaluation questions, and are typically the more heavily weighted and most commonly answered questions of our evaluation. Therefore, the privacy overall score may serve as a proxy for how the application or service would likely score against its peers overall, after answering transparently only about half of our total evaluation questions. Figure 39 illustrates the strong linear relationship of an application or service's overall score and privacy overall score.

OVERALL SCORE VERSUS PRIVACY CONCERN OVERALL SCORE

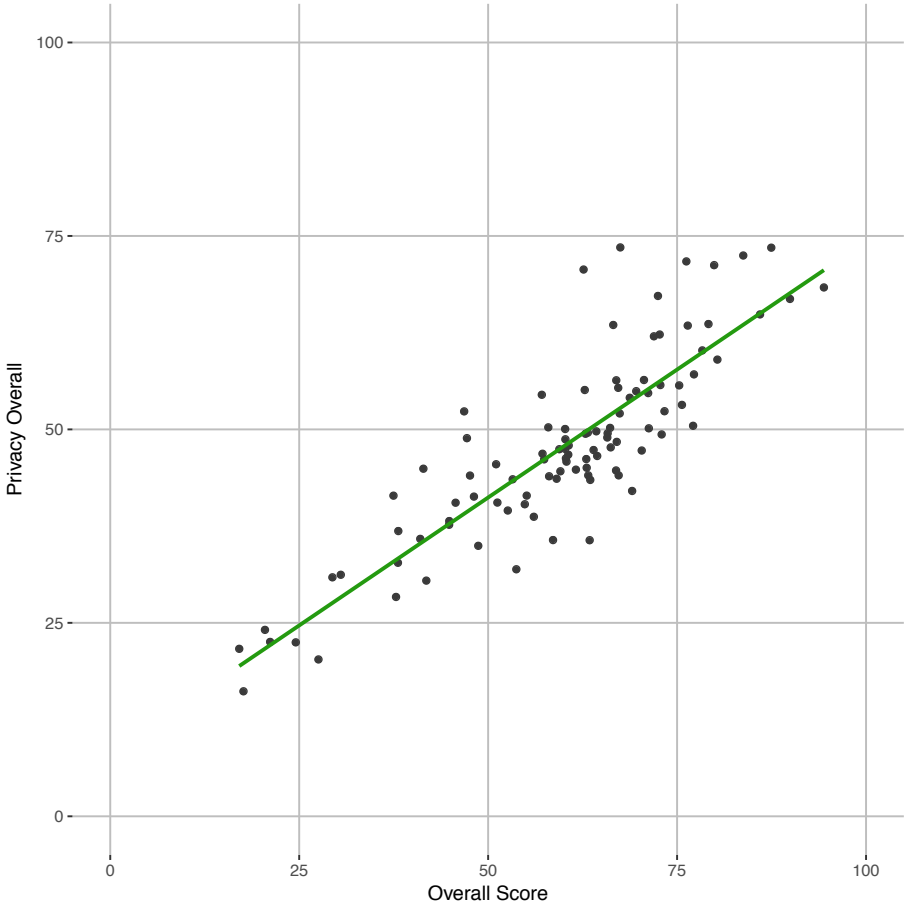


Figure 39: This chart illustrates the correlation between overall score and privacy overall score for the concern of privacy.

Collect PII

Among the applications or services we evaluated, approximately 92 percent disclosed that they collect personally identifiable information (PII). In addition, approximately 6 percent disclosed not-expected responses. Although not inherently a qualitatively worse practice, the collection of personal information from children or students is not always necessary in order to use the application or service as intended and may be qualitatively better or worse in context. However, the collection of personal information from children and students increases the risk that the information may inappropriately be used or disclosed. Collection of personal information also raises additional compliance challenges for vendors regarding the use, protection, and disclosure of that

personal information to third parties.[81, 82, 83, 84, 85] For purposes of this evaluation, we recommend that applications and services intended for children under 13 years of age and students not collect any personal information if possible, or limit their collection of information. Accordingly, applications and services can provide children or students with pseudonyms and limit the collection of personal information to only information required to use the product and where necessary to contact parents and teachers for consent. In context, it is understood that not all applications and services are the same. For example, a formative assessment application or service would need to collect more personal information than an online calculator application. However, the practice of collecting personal information can be mitigated to some extent, as explained in our later analysis of collection limitation.

PRIVACY: COLLECT PII

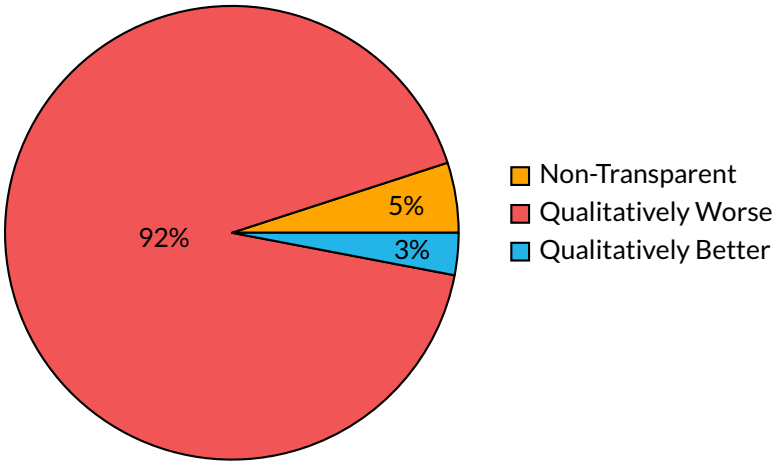


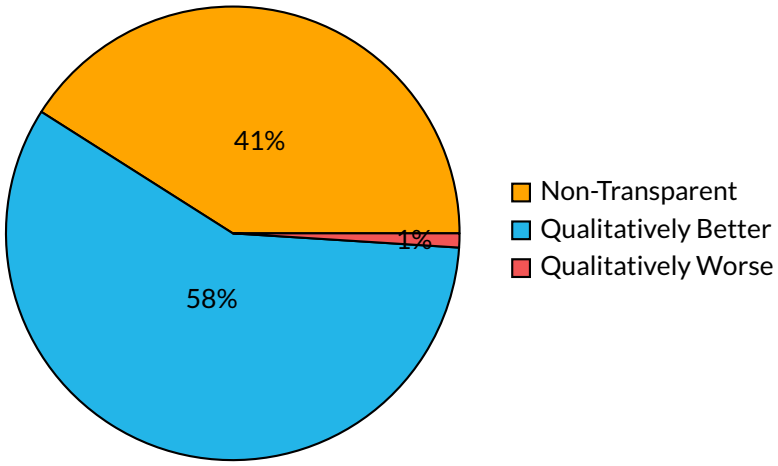
Figure 40: This chart illustrates the percentage of question responses about collecting PII. Qualitatively better question responses indicate the application or service does not collect personally identifiable information (PII). Qualitatively worse question responses indicate the application or service does collect personally identifiable information (PII). Non-transparent responses indicate the terms are unclear about whether or not the application or service collects personally identifiable information (PII).

Collection Limitation

Among the applications or services we evaluated, approximately 58 percent disclosed that they limit the collection or use of information to only data that are specifically required to use the application or service. In addition, approximately 5 percent disclosed not-expected responses. However, as compared to the Collect PII section, there

is a notable difference in the percentage of those applications and services that collect personal information but do not also limit their collection of that personal information. Approximately 41 percent of applications and services were non-transparent on this issue, which is surprising given that the more types of personal information collected, the more compliance obligations vendors need to navigate in their use, protection, and disclosure of that information.[86, 87, 88] However, from our analysis, we observationally determined many applications and services that are otherwise non-transparent on this issue collect very few personal information-data types and therefore engage in qualitatively better practices.

PRIVACY: COLLECTION LIMITATION



81 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 ("personally identifiable tnformation" under COPPA includes first and last name, photos, videos, audio, geolocation information, persistent identifiers, IP address, cookies, and unique device identifiers).

82 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.6(a)(2) (a parent or guardian can request the operator to provide a description of the specific types or categories of personal information collected from children by the application or service).

83 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22577(a)(1)–(6) (the term "personally identifiable information" under CalOPPA means individually identifiable information about a consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: 1). a first and last name; 2). a home or other physical address, including street name and the name of a city or town; 3). an email address; 4). a telephone number; 5). a Social Security number; or 6). any other identifier that permits the physical or online contacting of a specific individual).

84 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1 ("personal information" under FERPA includes direct identifiers such as a student or family member's name or indirect identifiers such as a date of birth or mother's maiden name or other information that is linkable to a specific student and that would allow a reasonable person in the school community to identify the student with reasonable certainty).

85 *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(1).

86 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.7 (a vendor is prohibited from conditioning a child's participation in a game or prize on the child disclosing more information than necessary to participate in the activity).

87 *See supra* note 36.

88 *See* General Data Protection Regulation (GDPR), Principles relating to processing of personal data, Art. 5(1)(c).

Figure 41: This chart illustrates the percentage of question responses about collection limitation. Qualitatively better question responses indicate the application or service limits the collection or use of information to only data that are specifically required to use the application or service. Qualitatively worse question responses indicate the application or service does not limit the collection or use of information to only data that are specifically required to use the application or service. Non-transparent responses indicate the terms are unclear about whether or not the application or service limits the collection or use of information to only data that are specifically required to use the application or service.

Data Shared

Among the applications or services we evaluated, approximately 90 percent disclosed a transparent response that collected information is shared with third parties. This practice is neither qualitatively better nor worse, because data can be shared with partners, affiliates, or third-party service providers with the same contractual obligations as the vendor's policies on its use. This question's purpose is to provide insight into the correlation between collecting and sharing data. As illustrated in the Collect PII section, a similar percentage of applications and services that disclose they collect personal information also disclose they share that information with third parties. This finding is not unexpected and further supports the assumption that any application or service that collects personal information also likely shares that information with third parties.

However, it is important that applications and services are aware that disclosure of child or student personal information raises additional compliance obligations.[89, 90, 91, 92, 93, 94, 95, 96] Other responses to this question included non-transparent disclosures, likely because no personal information is collected and thus could be shared with third parties or no third-party services are required to provide the service. Therefore, it is important, given the expectation that collected information is almost always shared with third parties, that vendors clearly describe the categories, names, and purposes of the third parties with which the application or service shares child or student information.

---

89 *See supra* note 40.

90 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (an operator may share data with third parties who provide support for the "internal operations" of the service and who do not use or disclose the information for any other purpose).

91 *See supra* note 65.

92 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(a)(2) (a parent is required to have the ability to consent to the collection and use of their child's personal information without also consenting to the disclosure of the information to third parties).

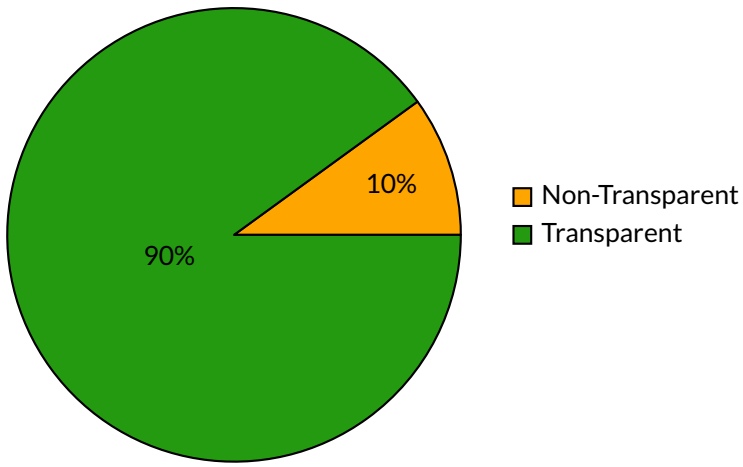


Figure 42: This chart illustrates the percentage of question responses about data shared. Transparent question responses indicate collected information is shared with third parties. Non-transparent responses indicate collected information is not shared with third parties.

Purpose Limitation

Among the applications or services we evaluated, approximately 72 percent disclose that the application or service limits the use of data to the educational purpose for which it was collected. In addition, approximately 5 percent disclosed not expected responses. This is an important issue for parents, teachers, schools, and districts, who expect that a majority of applications and services would be transparent and discuss qualitatively better practices on this issue. These practices also serve to mitigate our findings about collecting PII; approximately 92 percent of applications or services disclose they collect personal information. However, as compared to the Collect PII section, there is a notable percentage difference of approximately 20 percent for those applications and services that disclose they collect personal information but do not also disclose they limit their use of that personal information to the purpose for which it was collected. This difference of non-transparent qualitatively worse disclosures may

93 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30 (a school is prohibited from disclosing a student's "education record" or data to third parties without parental consent).

94 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(b)(4) (an operator is prohibited from sharing student information with third parties except in limited circumstances to other schools or for research purposes).

95 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(b)(4)(B)(C)(k) (an operator is prohibited from sharing student information with third parties except in limited circumstances to ensure legal and regulatory compliance; respond to or participate in a judicial process; or protect the safety of users, others, or the security of the site).

96 *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(10).

result in applications or services violating several federal or state laws if appropriate protections are not put in place.[97, 98, 99, 100, 101, 102]

It is likely that some of the approximately 20 percent of applications or services that have non-transparent responses to this question and collect personal information also limit the use of that information to the educational purpose for which it was collected but do not disclose that practice in their policies. In contrast, approximately 8 percent of applications and services disclosed qualitatively worse practices, likely because vendors do not believe their services will be used by children or students and therefore believe they are not required to disclose any limitations on their use of collected information.

PRIVACY: PURPOSE LIMITATION

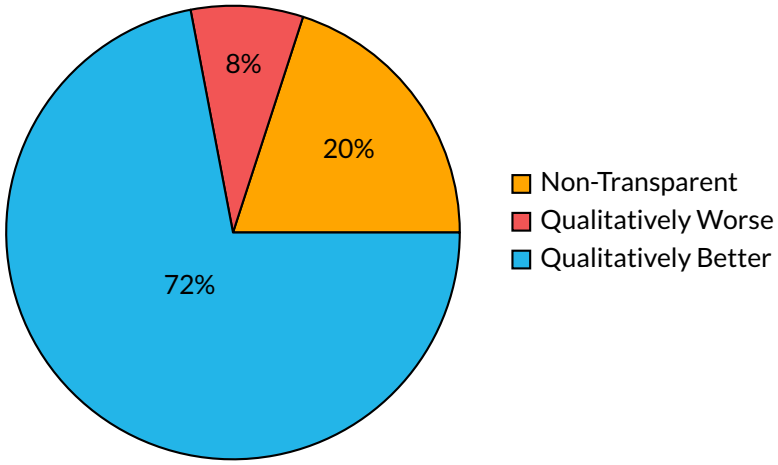


Figure 43: This chart illustrates the percentage of question responses about purpose limitation. Qualitatively better question responses indicate the application or service does limit the use of data collected to the educational purpose for which it was collected. Qualitatively

97 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10 (an operator may retain information collected from a child only as long as necessarily to fulfill the purpose for which it was collected and must delete the information using reasonable measures to prevent unauthorized use).

98 *See supra* note 90.

99 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(b) (an operator is required to provide direct notice to parents describing what information is collected, how information is used, its disclosure practices, and exceptions).

100 *See supra* note 66.

101 California AB 1584 Privacy of Pupil Records, Cal. Ed. Code §49073.1(b)(3) (a local educational agency that enters into a contract with a third party must ensure the contract contains a prohibition against the third party using any information in the pupil record for any purpose other than those required or specifically permitted by the contract).

102 *See* General Data Protection Regulation (GDPR), Principles relating to processing of personal data, Art. 5(1)(b); General Data Protection Regulation (GDPR), Data protection by design and by default, Art. 25(2).

worse question responses indicate the application or service does not limit the use of data collected to the educational purpose for which it was collected. Non-transparent responses indicate the terms are unclear about whether or not the application or service limits the use of data collected to the educational purpose for which it was collected.

Data De-identified

Among the applications or services we evaluated, approximately 66 percent disclose that the application or service shares information with third parties in an anonymous or de-identified format. This is an important exception to the prohibition on sharing child or student personal information with third parties. As compared to the Data Shared section, there is a difference of approximately 24 percent of applications and services that disclose they share data with third parties and those that disclose collected information is only shared in an anonymous or de-identified format. Sharing collected information in an anonymous or de-identified format is considered qualitatively better in our evaluation process, because given the expectation that collected information is shared with third parties, sharing information in a format that is not personally identifiable to the individual to whom the data belongs ultimately protects that child or student from their personal information being used by unauthorized individuals and from potential re-identification. However, this qualitatively better finding is lower than expected, given applications and services should clearly disclose in their policies that they only share child or student personal information with third parties that has been de-identified. Disclosing how information is shared with third parties provides parents and teachers with more information so they can make an informed decision about whether to use an application or service, and it is a critical issue for vendors to disclose in order for them to remain in compliance when sharing data with third parties for non-educational purposes.[103, 104, 105, 106, 107] In addition, approximately 5 percent of

---

103 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (an operator may disclose personal information collected from children to third parties if the data is not in an identifiable form such as de-identified, aggregated, or anonymous information).

104 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(b)(1) (an exception for disclosing personally identifiable information without obtaining parental consent exists for sharing "de-identified" student records where the educational institution has made a reasonable determination that a student's identity is not personally identifiable).

105 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(f)–(g) (an operator may share student information with a third party if in an aggregated or de-identified format).

106 California Privacy of Pupil Records, Cal. Ed. Code §49074 (a school district may provide, in its discretion, statistical data from which no pupil may be identified to any public agency, entity, private nonprofit college, university, or educational research and development organization when disclosure would be in the best educational interests of pupils).

107 *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(5); General Data Protection Regulation (GDPR), Data protection by design and by default, Art. 25(1).

applications and services disclosed qualitatively worse practices that they do not share personal information with third parties in an anonymous or de-identified format, likely because their policies typically define a broader range of company partners, affiliates, and transactional companies in which they share only personal information.

However, approximately 29 percent of applications and services evaluated were non-transparent on this issue, likely because they do not share child or student data in anonymized or de-identified formats for non-educational purposes and do not disclose practices they do not otherwise engage in. In context, there is no real accountability when an application or service's policies are non-transparent on this issue, because without transparent qualitatively better disclosures describing how personal information is de-identified with a reasonable level of justified confidence, it is not possible for parents, teachers, schools, or districts to verify whether child or student data is handled properly when shared with third parties.

PRIVACY: DATA DE-IDENTIFIED

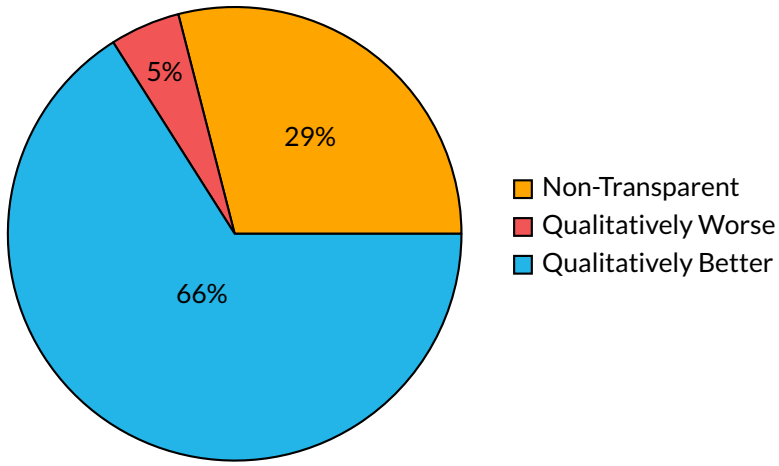


Figure 44: This chart illustrates the percentage of question responses about de-identified data. Qualitatively better question responses indicate the application or service does disclose information to third parties in an anonymous or de-identified format. Qualitatively worse question responses indicate the application or service does not disclose information to third parties in an anonymous or de-identified format. Non-transparent responses indicate the terms are unclear about whether or not the application or service discloses information to third parties in an anonymous or de-identified format.

Security Indicators

Among the applications or services we evaluated, the concern of security primarily examines practices wherein children's or students' information is protected with reasonable security measures based on industry best practices of encryption, two-factor authentication, and notice in the event of a data breach.

Security Transparency

Figure 45 illustrates the frequency of security transparency scores among all applications and services evaluated for the concern of security. From the analysis, we determined a mean of approximately 66/100. This mean is lower than expected, given that these applications and services are intended for children and students, but is similar to the mean for the Privacy Transparency section. From the analysis, it appears that the vast majority of applications and services at least disclosed they use reasonable security practices. In addition, because there are only 12 primary security concern questions, it is expected that security transparency scores would be concentrated at the higher end of the transparency scale within a smaller range.

SECURITY TRANSPARENCY

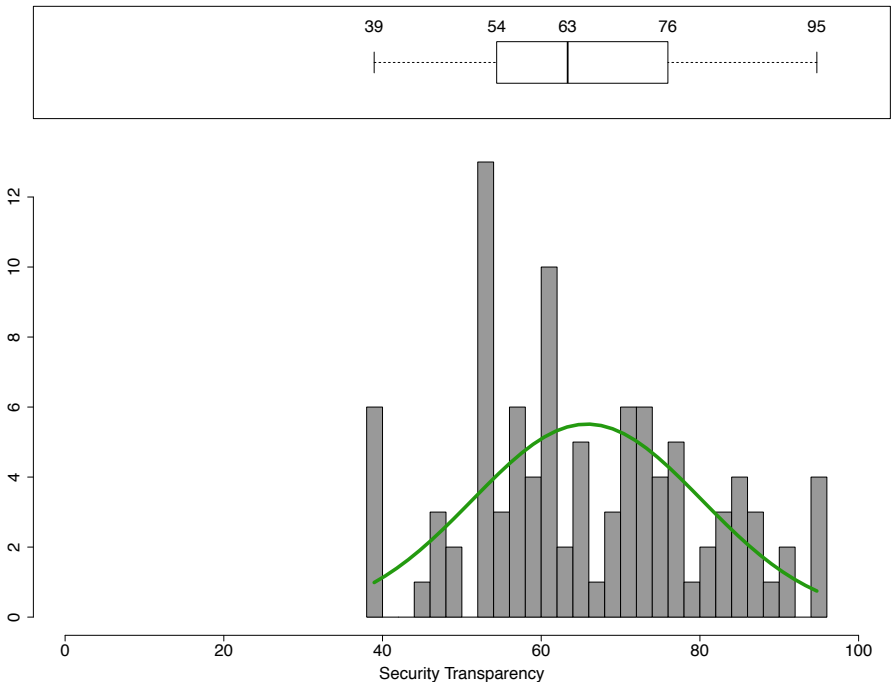


Figure 45: This chart illustrates the security transparency score distribution histogram and normal curve with median (Q2) 63, lower quartile (Q1) 54, upper quartile (Q3) 76, lower whisker 39 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 95 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Security Quality

Figure 46 illustrates the frequency of security quality scores among all applications and services evaluated for the concern of security. From the analysis, we determined a mean of approximately 73/100. However, the mean for security quality scores is not necessarily a strong indicator of overall practices, because there is a wide distribution in the range of extremely low scores that include several outliers and a concentration of extremely high quality scores. This finding is consistent with transparency and quality scores, wherein applications and services that are more transparent about security-concern-related questions are more likely to disclose qualitatively better practices. Therefore, although there is not likely enough data collected about this concern to make further determinations about overall trends, it appears generally there is a clear divide in quality between vendors who have better security practices and those with worse practices.

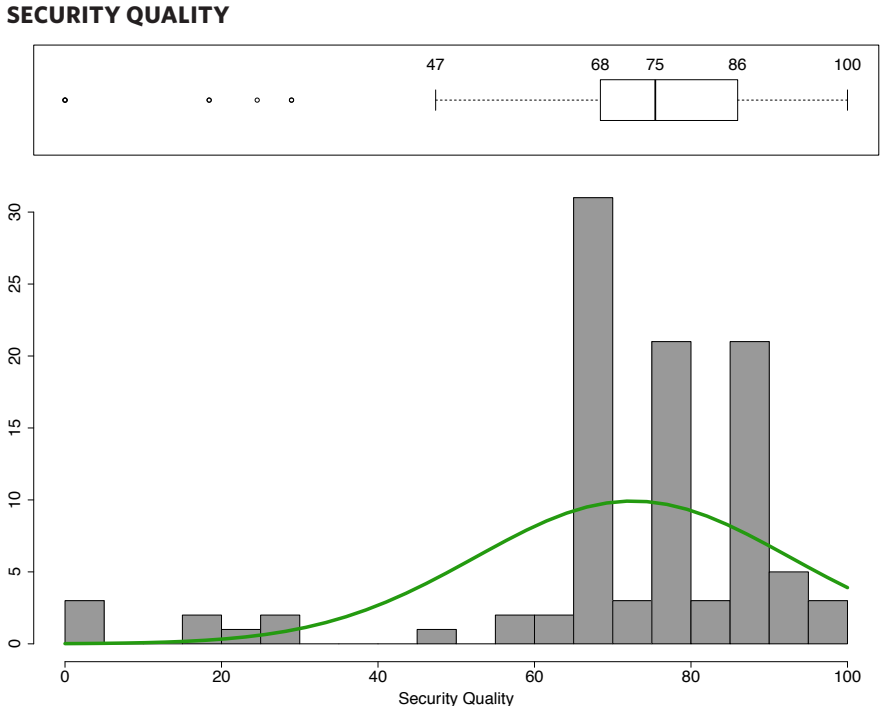


Figure 46: This chart illustrates the security quality score distribution histogram and normal curve with median (Q2) 75, lower quartile (Q1) 68, upper quartile (Q3) 86, lower whisker 47 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 100 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Security Overall Score

Figure 47 illustrates the frequency of security overall scores among all applications and services evaluated for the concern of security. From the analysis, we determined a mean of approximately 52/100. Similarly to the Security Transparency and Security Quality sections, this mean is lower than expected, given that the services evaluated are intended for children and students. However, as compared to the Security Quality section, the range of security overall scores better illustrates a normal distribution of comparative scores given the high frequency of transparency scores in the high score range. Therefore, the security overall score is a strong indicator of how applications and services protect child and student information and should help parents, teachers, schools, and districts differentiate among products based on their respective security practices.

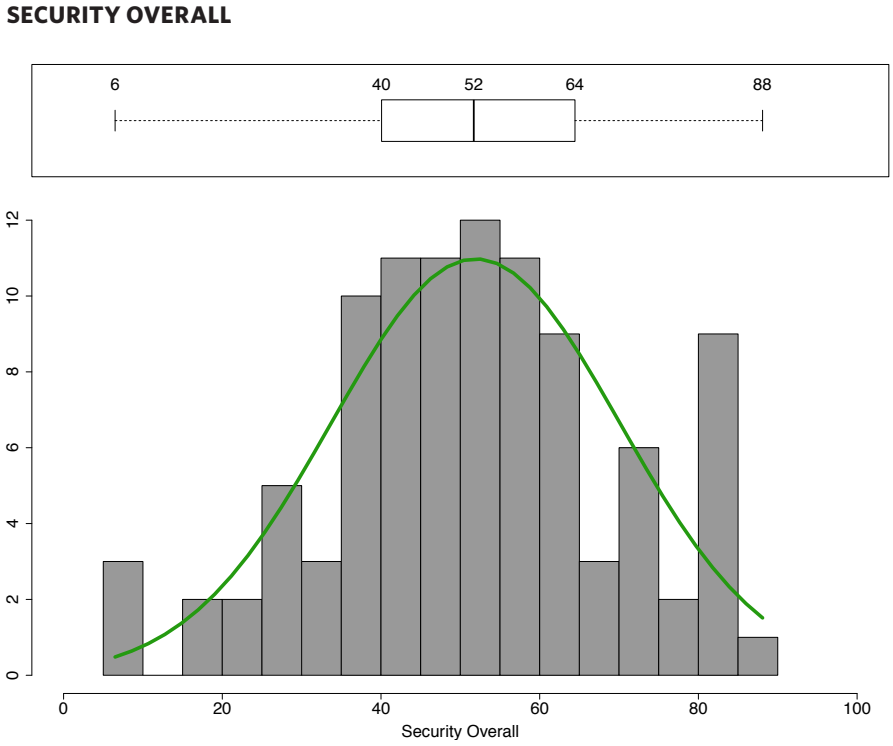


Figure 47: This chart illustrates the security overall score distribution histogram and normal curve with median (Q2) 52, lower quartile (Q1) 40, upper quartile (Q3) 64, lower whisker 6 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 88 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Two-Factor Authentication

Among the applications or services we evaluated, approximately 37 percent disclosed that the application or service provides two-factor authentication. This percentage is lower than expected, but the adoption of two-factor authentication as a reasonable security industry standard is relatively new and has been steadily increasing year over year as more edtech applications and services adopt this qualitatively better practice. Accordingly, two-factor authentication is a qualitatively better practice, because, as compared to other more complex security tools, it is considered easier to understand and implement with parents, teachers, and students who already have a mobile device and are familiar with receiving text messages and using mobile applications. In addition, two-factor authentication can be integrated relatively quickly into applications and services and provides a relatively high level of security compared to the low cost to implement. These additional security protections can help prevent unauthorized access to children's and students' accounts and minimize the risk of potential data breaches.

In order to gain access to an authenticated system with two-factor authentication, an attacker must know both the user's username and password and must also have access to a second factor to authenticate. Children and students can no longer rely on a single password or commonly used security questions to secure all their online accounts. Answers to identity-based questions can be discovered, and passwords are easy to lose or steal, especially if passwords are used with more than one online service. Moreover, children's and students' email addresses often serve as the master key to all the other online services they use. If a user's email password is compromised, then all the other services they use could also be at risk. This is why providing two-factor authentication is such an important security practice for the applications and services we evaluated. However, approximately 63 percent of applications and services are non-transparent on this issue, which indicates the industry still has a long way to go in adopting this important information-security technology.

SECURITY: TWO-FACTOR AUTHENTICATION

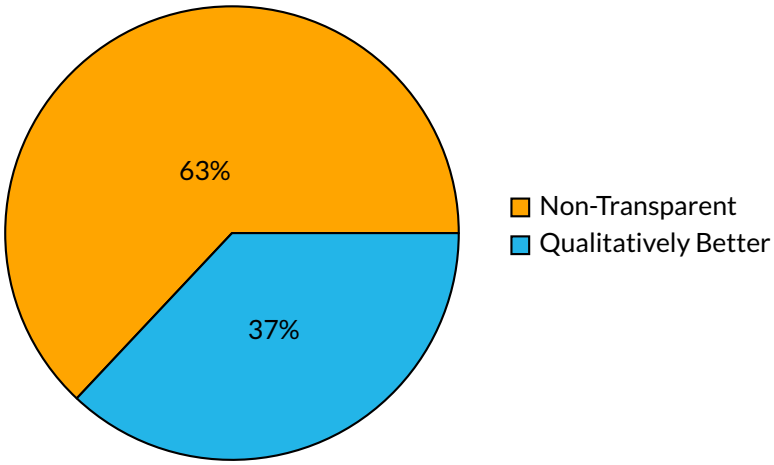


Figure 48: This chart illustrates the percentage of question responses about two-factor authentication. Qualitatively better question responses indicate the application or service provides two-factor authentication. Non-transparent responses indicate the terms are unclear about whether or not the application or service provides two-factor authentication.

Reasonable Security

Among the applications or services we evaluated, approximately 92 percent disclosed a qualitatively better response that reasonable security standards are used to protect the confidentiality of a child or student's personal information. Accordingly, using reasonable security standards to protect collected information is considered qualitatively better in our evaluation process, because it includes security methods that protect children's and student's information against unauthorized access or inadvertent disclosure that could cause serious harm.[108, 109] Reasonable security measures are a subjective determination of industry standards based on the type of application or service and the context in which it is used. For example, a student-assessment application used in classrooms and that collects extensive personal and behavioral information would require different reasonable security measures from an online calculator that collects little or no personal information. Determining the level of reasonable security to adequately protect child and student information requires each vendor to perform an internal and external privacy assessment to determine the type and amount of information

108 *See supra* notes 34–38, 65.

109 *See* General Data Protection Regulation (GDPR), Principles relating to processing of personal data, Art. 5(1)(f); General Data Protection Regulation (GDPR), Security of processing, Art. 32(1)(b), 32(2).

collected and shared. Furthermore, approximately only 8 percent of applications and services evaluated were non-transparent on this issue, which may be attributable to products that collect little or no personal information and therefore do not disclose use of reasonable security measures to protect information they do not otherwise collect.

SECURITY: REASONABLE SECURITY

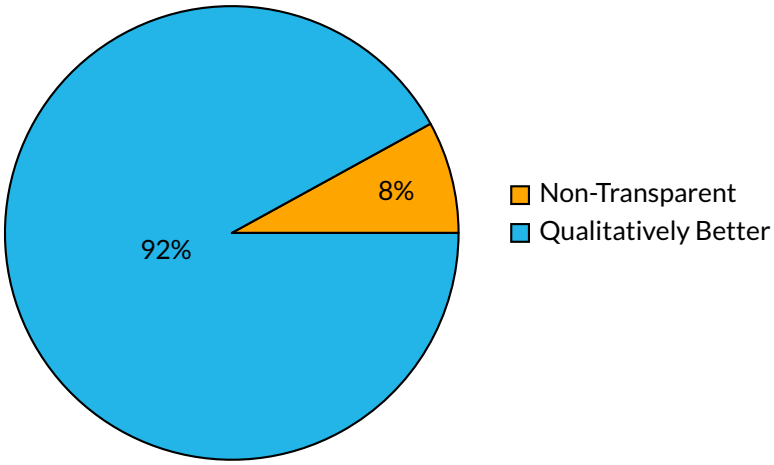


Figure 49: This chart illustrates the percentage of question responses about reasonable security. Qualitatively better question responses indicate the application or service provides reasonable security standards to protect the confidentiality of personal information. Non-transparent responses indicate the terms are unclear about whether or not the application or service provides reasonable security standards to protect the confidentiality of personal information.

Transit Encryption

Among the applications or services we evaluated, approximately 40 percent disclosed that collected information is encrypted while in transit to protect the confidentiality of a child or student's information. This percentage is lower than expected, given encrypting information transmitted online is considered an industry best practice and reasonable security standard. In addition, approximately 57 percent disclosed not-expected responses. In contrast, approximately 92 percent of applications and services disclosed they engaged in the qualitatively better practice of reasonable security, which includes encrypting transmitted information. However, we observed that the majority of applications and services evaluated do in fact use encryption of information transmitted online, such as secure sockets layer (SSL) or transport layer security (TLS), but do not

disclose this standard security practice in their policies. Moreover, approximately 56 percent of applications and services were non-transparent about whether they provide encryption of information in transit, and approximately 4 percent indicated they do not provide encryption of transmitted information. The higher-than-expected percentage of non-transparent responses on this issue is likely attributable to the general assumption that because an application or service already discloses they provide reasonable security, they are not also required to disclose the particular details of those reasonable security practices. However, applications and services are recommended to be more transparent on this issue, given both federal and state compliance obligations exist to protect child and student data with reasonable security standards that require notice of compliance.[110, 111, 112]

SECURITY: TRANSIT ENCRYPTION

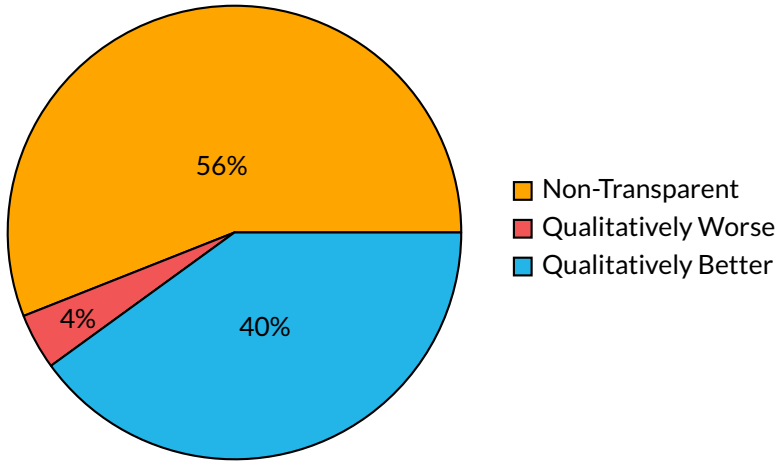


Figure 50: This chart illustrates the percentage of question responses about transit encryption. Qualitatively better question responses indicate collected information is encrypted while in transit. Qualitatively worse question responses indicate collected information is not encrypted while in transit. Non-transparent responses indicate the terms are unclear about whether or not collected information is encrypted while in transit.

110 Common Sense Media, *Encryption Survey* (March 2017), https://www.commonsense.org/education/privacy/blog/encryption-survey-march-2017.

111 *See supra* notes 34–38, 65.

112 *See* General Data Protection Regulation (GDPR), Security of processing, Art. 32(1)(a).

Storage Encryption

Among the applications or services we evaluated, approximately 28 percent disclosed that collected information is encrypted while in storage to protect the confidentiality of a child or student's data. Similarly to the Transit Encryption section, this percentage is lower than expected, given encrypting information while stored is assumed to be an industry best practice and reasonable security standard, especially given the increased adoption of third-party cloud storage and hosting providers that provide encryption of collected information automatically. In addition, approximately 54 percent disclosed not-expected responses. Our evaluation process limits its analysis to the statements regarding storage encryption made in policies of applications and services that are publicly available prior to use. Therefore, the lower-than-expected percentage of qualitatively better responses may not reflect actual usage of storage encryption, because our evaluation process does not observationally determine whether collected information that was encrypted while in transit was also subsequently stored at rest with the vendor or third party in an encrypted or unreadable format.

In addition, approximately 70 percent of applications and services were non-transparent regarding whether they encrypt collected information while stored. This finding is unexpected given that both federal and state compliance obligations exist to protect child and student data with reasonable security standards of encrypting collected information while stored at rest. Encrypting collected information while it's in storage also serves to protect child and student information in the event of a data breach and removes potential data-breach-notification-compliance obligations on the vendor. [113, 114] Similarly to the Transit Encryption section, an additional approximately 14 percent of applications and services were not transparent in their policies whether they actually encrypt collected information in storage. Given our findings in the Reasonable Security section, this would indicate that a majority of non-transparent responses should disclose their qualitatively better practices of encrypting stored information, because they already disclose that they provide reasonable security protections of information collected from children and students.

---

113 *See supra* notes 34–38, 65.

114 *See* General Data Protection Regulation (GDPR), Security of processing, Art. 32(1)(a).

SECURITY: STORAGE ENCRYPTION

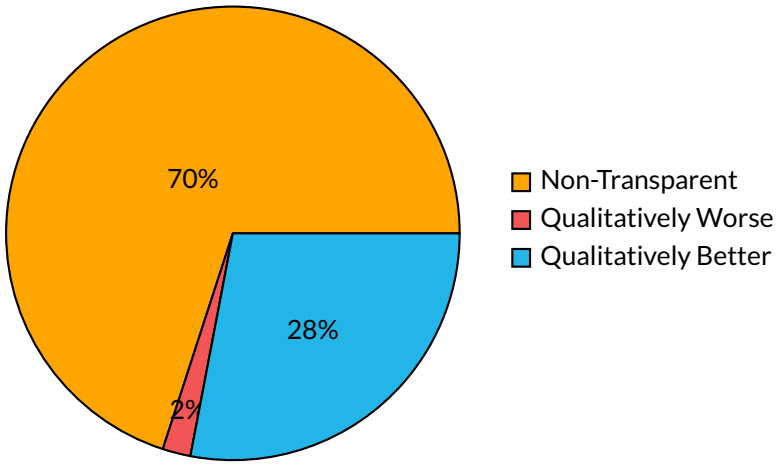


Figure 51: This chart illustrates the percentage of question responses about storage encryption. Qualitatively better question responses indicate collected information is encrypted while in storage. Qualitatively worse question responses indicate collected information is not encrypted while in storage. Non-transparent responses indicate the terms are unclear about whether or not collected information is encrypted while in storage.

Breach Notice

Among the applications or services we evaluated, approximately 36 percent disclosed that in the event of a data breach, if unencrypted collected information is disclosed to unauthorized individuals, that application or service will provide notice to any users affected. In addition, approximately 18 percent disclosed not-expected responses. Accordingly, providing notice to users that their unencrypted information has been disclosed is considered a qualitatively better practice in our evaluation and also required by various state laws.[115, 116, 117] However, approximately 6 percent of applications or services evaluated disclosed that they do not provide notifications in the event of a data breach, which is a qualitatively worse practice in our evaluation process. This is likely attributable to vendors disclosing they are not legally responsible for providing data-breach notifications to

115 California Data Breach Notification Requirements, Cal. Civ. Code §1798.29, §1798.29(h)(4), §1798.82 (a business that collects personal information from California consumers is required to disclose a breach of the security of their system following discovery or notification of the breach in the security of a consumer's data whose unencrypted personal information was reasonably believed to have been acquired by an unauthorized person).

116 California AB 1584 Privacy of Pupil Records, Cal. Ed. Code §49073.1(b)(6) (a local educational agency that enters into a contract with a third party must ensure the contract contains a description of the procedures for notifying the affected parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil's records).

117 *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(12); General Data Protection Regulation (GDPR), Notification of a personal data breach to the supervisory authority, Art. 33(1)–(5); General Data Protection Regulation (GDPR), Communication of a personal data breach to the data subject, Art. 34(1)–(3).

users in the event their collected information is disclosed to unauthorized individuals, because any breach would have to originate with their third-party service provider and not themselves. However, it is recommended that applications and services transparently explain their data-breach-notification policies and any contractual obligations of third-party service providers who may be providing notification to users on behalf of the company to ensure parents, teachers, schools, and districts are adequately notified.

Moreover, approximately 58 percent of applications and services evaluated were non-transparent on this issue, which is unexpected given that a majority of U.S. states have data-breach-notification-compliance obligations that vendors are required to follow.[118] Similarly to non-transparent behavior on other issues, vendors likely believe that disclosing their qualitatively better practices of data-breach notification may in fact introduce unnecessary liability if they are unable to adequately notify affected users within the specified time frame. However, it is recommended that applications and services increase their transparency on this important issue in order to communicate their data-breach-response-and-notification process to parents, teachers, schools, and districts. Providing notice of this process will allow affected users to more quickly and adequately respond and protect themselves in the event of a data breach.

SECURITY: BREACH NOTICE

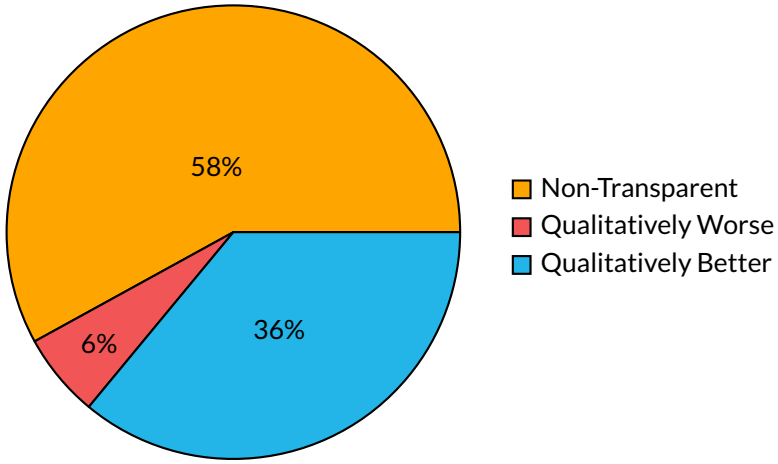


Figure 52: This chart illustrates the percentage of question responses about breach notices. Qualitatively better question responses indicate notice is provided to affected users if their unencrypted collected information is disclosed to unauthorized individuals in a data breach. Qualitatively worse question responses indicate that no notice is provided to affected users if their unencrypted collected information is disclosed to unauthorized individuals in a data breach. Non-transparent responses indicate the terms are unclear about whether or not notice is provided to affected users if their unencrypted collected information is disclosed to unauthorized individuals in a data breach.

Compliance Indicators

Among the applications or services we evaluated, the concern of compliance primarily examines practices wherein information from children under 13 years of age and students are collected and used under federal laws such as the Children's Online Privacy Protection Act (COPPA)[119] and the Family Education Records and Privacy Act (FERPA)[120] and state laws such as the Student Online Personal Information Protection Act (SOPIPA)[121].

Compliance Transparency

Figure 53 illustrates the frequency of compliance transparency scores among all applications and services evaluated for the concern of compliance. From the analysis, we determined a mean of approximately 51/100. This mean is lower than expected, given that these applications and services are intended for children and students and therefore are expected to have more child- and student-related compliance disclosures. However, this wide distribution range of transparency scores from 58 compliance-concern questions illustrates that vendors are likely to only disclose qualitatively better compliance-related practices they believe are selectively relevant to their applications or services. This lack of transparency often creates confusion for parents, teachers, and districts, who are unable to make informed decisions about whether to use an application or service because it is unclear whether it meets all the compliance obligations required for collecting, using, and disclosing children's and students' personal information.

118 National Conference of State Legislatures, *Security Breach Notification Laws* (Feb. 6, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breachnotification-laws.aspx.

119 *See supra* note 11.

120 *See supra* note 13.

121 *See supra* note 12.

COMPLIANCE TRANSPARENCY

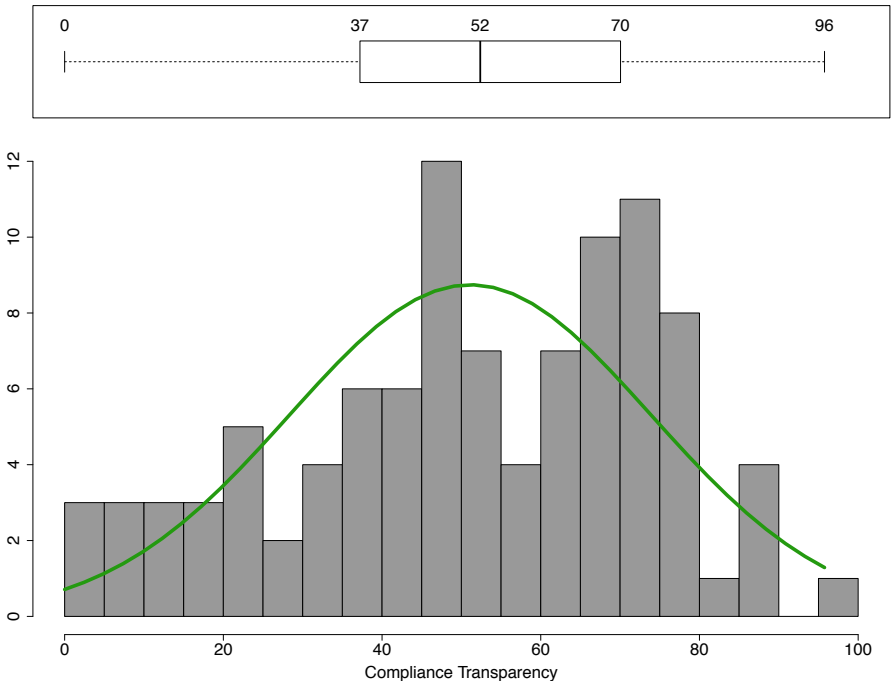


Figure 53: This chart illustrates the compliance transparency score distribution histogram and normal curve with median (Q2) 52, lower quartile (Q1) 37, upper quartile (Q3) 70, lower whisker 0 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 96 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Compliance Quality

Figure 54 illustrates the frequency of compliance quality scores among all applications and services evaluated for the concern of compliance. From the analysis, we determined a mean of approximately 60/100. Similarly to the Compliance Transparency section, this mean is lower than expected, given that the applications and services evaluated are intended for children and students. However, the majority of quality scores are concentrated in a high score band between 50 and 90, which indicates that transparent disclosures are more likely to be qualitatively better. Where we see quality scores fall below 50, these applications or services typically only disclose broad language that they comply with federal children and student data-collection laws such as COPPA and FERPA but do not otherwise provide any substantive information explaining which practices they actually take part in to obtain compliance.

COMPLIANCE QUALITY

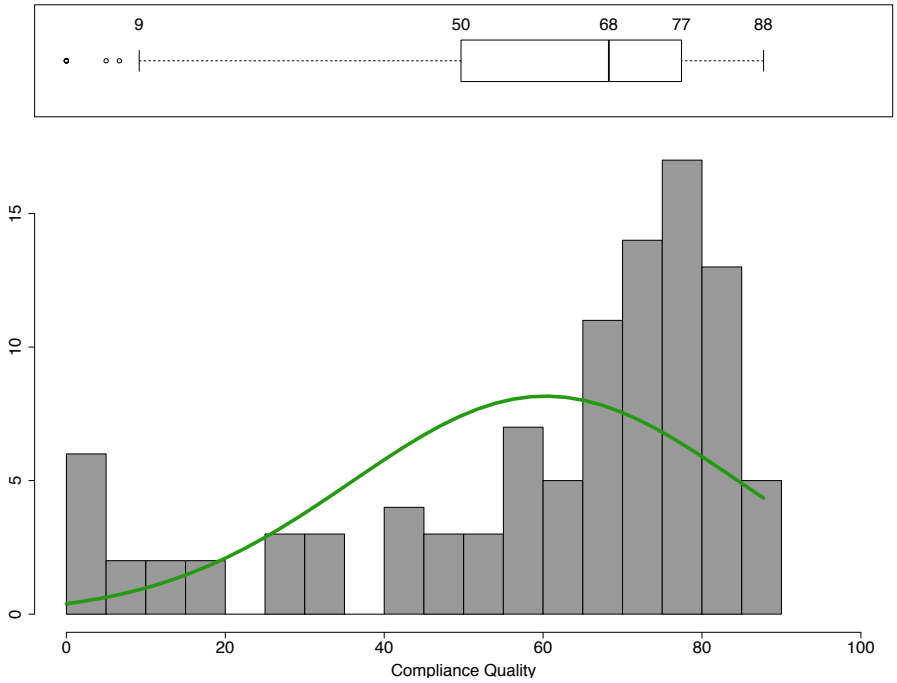


Figure 54: This chart illustrates the compliance quality score distribution histogram and normal curve with median (Q2) 68, lower quartile (Q1) 50, upper quartile (Q3) 77, lower whisker 9 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 88 (largest datum within Q3 + 1.5 x IQR). Any outliers are denoted by circles outside the whiskers.

Compliance Overall Score

Figure 55 illustrates the frequency of compliance overall scores among all applications and services evaluated for the concern of compliance. From the analysis, we determined a mean of approximately 38/100. Similarly to the Compliance Transparency and Compliance Quality sections, this mean is significantly lower than expected, given that the applications and services evaluated are intended for children and students. However, the range of overall scores are skewed to a lower bound of 0, because many general audience consumer-focused applications and services disclose they are not directed or targeted to students or children under 13 years of age and therefore are non-transparent on all compliance-related questions.

However, these applications and services likely would still appeal to children and students under 13 years of age and are currently among the 100 most popular educational applications and services used by children and students. These skewed findings are notable, because approximately 10 percent of all applications and services are

non-transparent about a majority of questions relating to expected-to-disclose compliance obligations for children and students. From our analysis, it appears most applications and services focus their transparent responses only on required-to-be-disclosed compliance obligations and remain non-transparent about important limitations or exceptions to those disclosures.[122, 123, 124, 125]

COMPLIANCE OVERALL

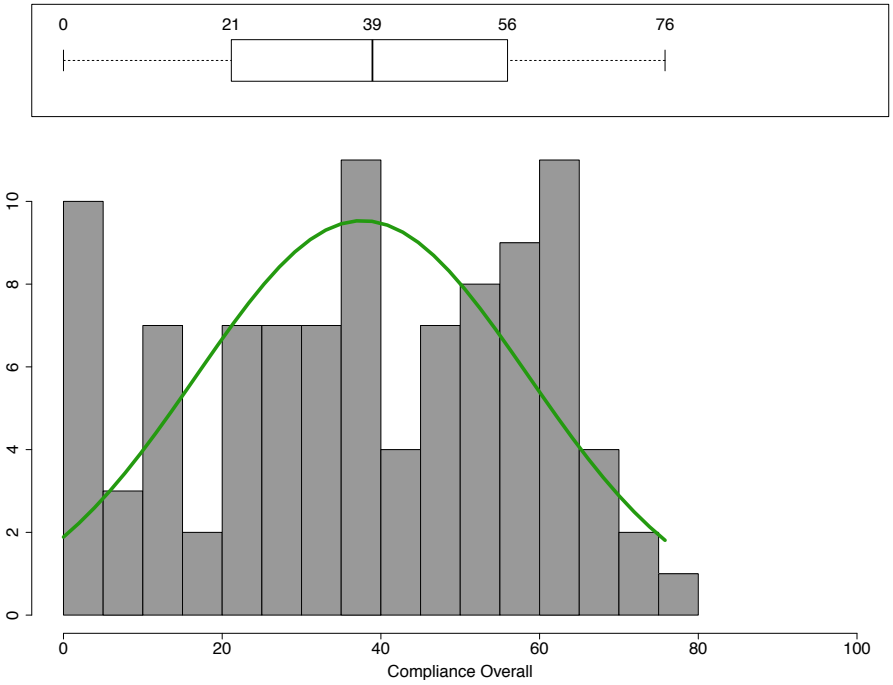


Figure 55: This chart illustrates the compliance overall score distribution histogram and normal curve with median (Q2) 39, lower quartile (Q1) 21, upper quartile (Q3) 56, lower whisker 0 (smallest datum within Q1 - 1.5 x IQR), and upper whisker 76 (largest datum within Q3 + 1.5 x QR). Any outliers are denoted by circles outside the whiskers.

122 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(1) (an exception to obtaining parental consent exists for an operator to collect a parent or child's information for the sole purpose of obtaining consent).

123 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(2) (An exception to obtaining parental consent exists for an operator to contact a parent and provide notice about a child's participation in the service).

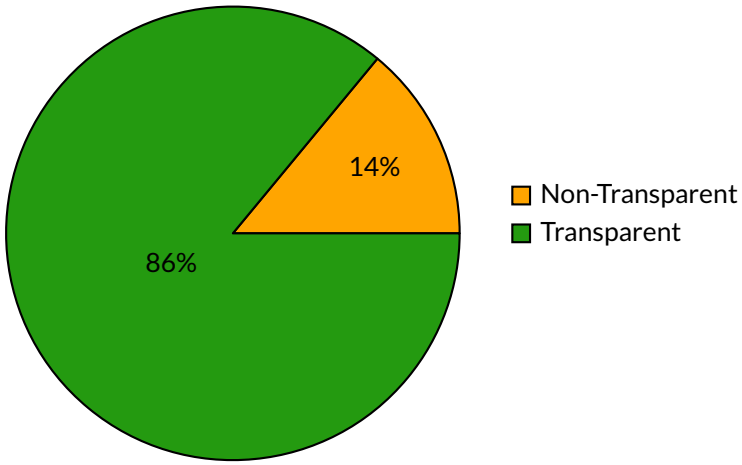
124 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(3)–(4) (an exception to obtaining parental consent exists for an operator to respond directly on a one-time basis, or more than once, to a specific request from a child or parent).

125 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(6); 34 C.F.R. Part 99.31(b)(2) (an exception for disclosing personally identifiable information without obtaining parental consent exists for sharing data with third parties conducting legitimate research and studies).

Children Intended

Among the applications or services we evaluated, approximately 86 percent disclosed that the applications or services are intended for children under 13 years of age. This high percentage is expected given that our evaluation process targeted 100 popular edtech applications and services used by children.[126] However, given our findings of a compliance overall score mean of only 36/100, there is clearly a compliance deficiency with regard to use by children under 13 years of age. It appears that given this low mean, a high percentage of applications and services that disclose they are intended for children under 13 do not also disclose expected compliance obligations for the collection, use, and disclosure of information from those children. Moreover, approximately 14 percent of applications and services were non-transparent about whether they are intended for children under 13 years of age. This finding is also observed in the compliance overall score, wherein general audience consumer-focused applications and services disclose they are not directed or targeted to children under 13 years of age but likely would still appeal to children under 13, which takes into account several factors.[127] Therefore, parents and teachers need to exercise caution when evaluating whether to use popular edtech applications or services, and vendors need to provide greater transparency about their collection, use, and disclosure practices around personal information from children under 13 years of age.

COMPLIANCE: CHILDREN INTENDED



126 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (a site directed to children is where the operator has actual knowledge the site is collecting information from children under the age of 13 and parental consent is required before any collection or use of information).

127 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (an exception for a general audience site exists if the site would appeal to children under 13 years of age, which would take into account several factors that include subject matter, visual content, age of models, and activities provided).

Figure 56: This chart illustrates the percentage of question responses about children intended. Transparent question responses indicate the application or service discloses it is intended to be used by children under the age of 13. Non-transparent responses indicate the application or service discloses it is not intended to be used by children under the age of 13.

Students Intended

Among the applications or services we evaluated, approximately 73 percent disclosed that the applications or services evaluated are intended for students. This high percentage is expected given that our evaluation process targeted 100 popular edtech applications and services used by students. Moreover, approximately 27 percent of applications and services were non-transparent about whether or not they are intended for students. This finding is also observed in the compliance overall score, wherein general audience consumer-focused applications and services disclose they are not directed or targeted to students but are still commonly used by teachers and students in preschool or K–12 classrooms. The approximately 13 percent greater occurrence of non-transparent responses to this question, as compared to the Children Intended section, is likely attributable to applications and services disclosing they are only intended for children, because they are under the assumption use by children inherently includes students. Similarly to the Children Intended section, parents and teachers need to exercise caution when evaluating whether to use popular edtech applications or services in the classroom, and vendors need to provide greater transparency about their collection, use, and disclosure practices around the personal information of students.[128, 129, 130, 131, 132]

---

128 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(a) (SOPIPA applies to operators of online services that are primarily used for K–12 school purposes and were designed and marketed for K–12 school purposes).

129 Early Learning Personal Information Protection Act (ELPIPA), Cal. B.&P. Code §22586(a)(1) (ELPIPA applies to operators of online services that are primarily used for preschool or pre-kindergarten purposes and were designed and marketed for preschool or pre-kindergarten purposes).

130 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §22584(m) (SOPIPA does not apply to general audience websites and services that are not primarily used by K–12 students).

131 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1 ("personal information" under FERPA includes direct identifiers such as a student or family member's name or indirect identifiers such as date of birth or mother's maiden name or other information that is linkable to a specific student and that would allow a reasonable person in the school community to identify the student with reasonable certainty).

132 California Privacy of Pupil Records, Cal. Ed. Code §49073.6 (prohibits schools, school districts, county offices of education, and charter schools from collecting or maintaining information about pupils from social media for any purpose other than school or pupil safety, without notifying each parent or guardian and providing the pupil with access and an opportunity to correct or delete such information).

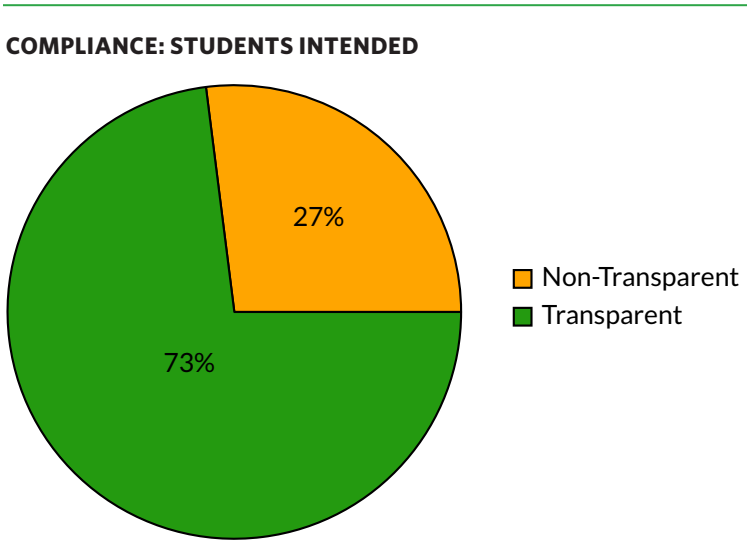


Figure 57: This chart illustrates the percentage of question responses about students intended. Transparent question responses indicate the application or service discloses it is intended for students. Non-transparent responses indicate the application or service discloses it is not intended for students.

School Purpose

Among the applications or services we evaluated, approximately 57 percent disclosed that the applications or services are primarily designed, marketed, and used for preschool or K–12 school purposes. However, there is an apparent discrepancy between the Students Intended section, where there is a difference of approximately 16 percent between applications and services that disclosed that students are the intended audience but did not also disclose the service is primarily designed, marketed, and used for preschool or K–12 school purposes. This suggests a small percentage of applications and services that disclose they are intended for students but only target higher education students over 18 years of age. However, this lack of transparency surrounding "school purpose" could create confusion with parents, teachers, schools, and districts about whether additional compliance obligations would be applicable to the application or service for students under 18 years of age, because of various state laws such as California's Student Online Personal Information Protection Act (SOPIPA).[133]

133 *See supra* notes 128–130.

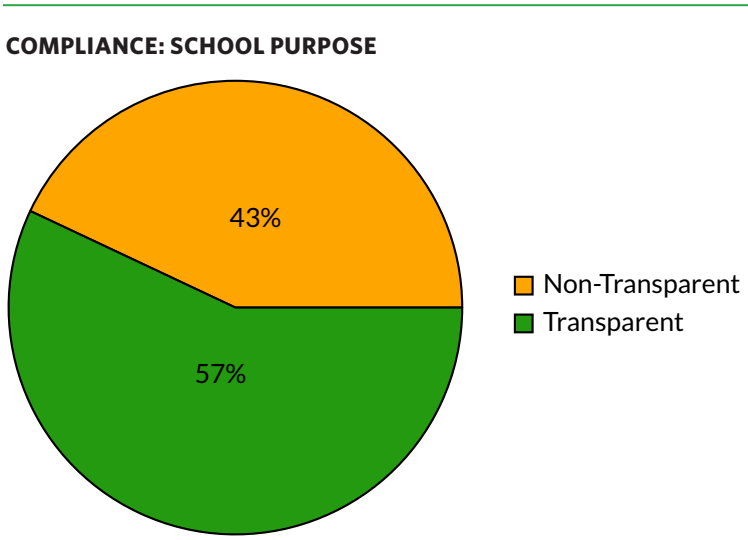


Figure 58: This chart illustrates the percentage of question responses about school purpose. Transparent question responses indicate the application or service discloses it is primarily designed, marketed, and used for preschool or K–12 school purposes. Non-transparent responses indicate the application or service discloses it is not primarily designed, marketed, and used for preschool or K–12 school purposes.

Parental Consent

Among the applications or services we evaluated, approximately 71 percent disclosed that verifiable parental consent must be obtained before they collect or disclose any child or student's personal information. This finding is lower than expected, likely because non-transparent applications and services assume they do not need to obtain parental consent if they disclose their service is not intended for children or students. However, given that approximately 57 percent of applications and services are directed at schools, as indicated in the School Purpose section, the percentage difference of transparent responses about parental consent may be attributable to additional student data privacy agreements that exist privately between the vendor and schools or districts that define the parental-consent collection process on behalf of the schools or districts.

In addition, as indicated in the Children Intended section, approximately 14 percent indicated they only provide general audience or mixed audience consumer-focused applications and services and therefore disclose they are neither directed nor targeted to children under 13 years of age. These applications and services require parental consent to be obtained only where the vendor has actual knowledge that a child under the age of 13 has registered an account or is using the service. However, these applica-

tions or services would still need to obtain parental consent, because they would likely appeal to children under the age of 13, which takes into account several factors, including that they are among 100 of the most popular edtech products used by children and students.[134, 135, 136, 137, 138, 139]

As indicated in both the Children Intended and Students Intended sections, it is assumed the approximately 14 percent, and 27 percent respectively of non-transparent responses from applications and services about whether they are collecting personal information from children or students under 13 years of age, are in fact collecting information from children and students without actual knowledge. Therefore, because these applications and services are likely being used by children and students without disclosing notice to parents or teachers that they need to provide verifiable parental consent, or that they obtain parental consent through additional student data privacy agreements with schools or districts, these applications and services may be in violation of federal law.[140, 141, 142, 143]

---

134 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (a general audience site is where the operator has no actual knowledge that a child under the age of 13 has registered an account or is using the service and no age gate or parental consent is required before collection of information).

135 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (a mixed audience site is where the site is directed to children but does not target children as its "primary audience" but rather teens 13 to 18 years of age or adults. An operator of a mixed audience site is required to obtain age information from a user before collecting any information, and if a user identifies themselves as a child under the age of 13, the operator must obtain parental consent before any information is collected).

136 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2 (a site directed to children is where the operator has actual knowledge the site is collecting information from children under the age of 13 and parental consent is required before any collection or use of information).

137 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(d) (a vendor who may obtain actual knowledge that it is collecting information from a child must not encourage a child from disclosing more information than reasonably necessary through an age-verification mechanism. An age gate should: be age-neutral; not encourage falsification; list day, month, and year; have no prior warning that under-13 children will be blocked; prevent multiple attempts).

138 *See supra* note 127.

139 *See* General Data Protection Regulation (GDPR), Conditions Applicable to Child's Consent in Relation to Information Society Services, Art. 8(1).

140 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5 (an operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children under 13 years of age).

141 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(1) (an operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology and existing methods available to a parent to prove their identity); *See* 15 U.S.C. §6501(9).

142 *See supra* note 93.

143 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30 (a parent or eligible student is required to provide signed and dated written consent before an educational institution discloses personally identifiable information from the student's record).

COMPLIANCE: PARENTAL CONSENT

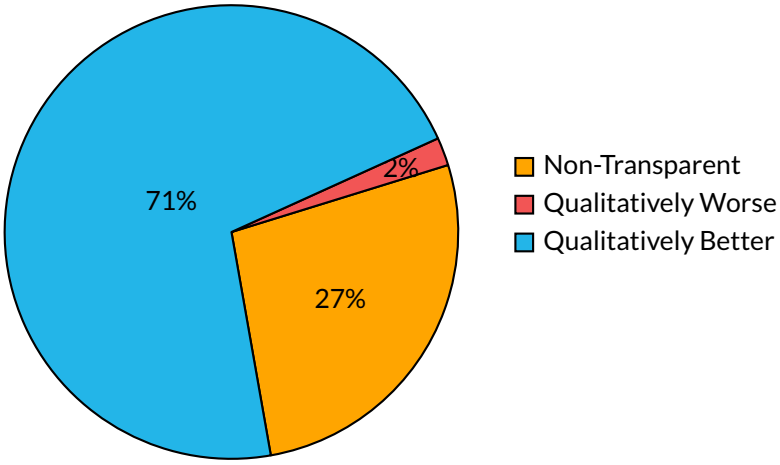


Figure 59: This chart illustrates the percentage of question responses about parental consent. Qualitatively better question responses indicate the application or service requires verifiable parental consent to be obtained before they collect or disclose any child or student's personal information. Qualitatively worse question responses indicate the application or service does not require verifiable parental consent to be obtained before they collect or disclose any child or student's personal information. Non-transparent responses indicate the terms are unclear about whether or not the application or service requires verifiable parental consent to be obtained before they collect or disclose any child or student's personal information.

Consent Method

Among the applications or services we evaluated, approximately 32 percent indicated the methods available to provide verifiable parental consent. This finding is extremely low given that these applications and services are intended for children under 13 years of age and students. Accordingly, a majority of approximately 65 percent do not provide any information about how parents or teachers can actually provide consent. From our analysis, this percentage is non-conforming with the Children Intended section, which indicated approximately 86 percent of applications and services evaluated are intended for children under 13 years of age, and with the Parental Consent section, which indicated approximately 71 percent of applications and services disclosed they obtain parental consent. However, we did observe applications and services that were non-transparent about the methods available to provide parental consent but otherwise provided a secondary parent or teacher account that used online methods to provide consent through the creation of an associated child or student account. This

unexpected behavior of non-transparency with otherwise qualitatively better practices is likely because these applications and services believe their parental consent methods to be self-evident.

However, these parent or teacher accounts could potentially be used as a means to collect personal or behavioral-related information from the parents and teacher themselves. This type of personal or behavioral information could be used for advertising purposes and even directed back to the parents and teachers for educational-related products that could potentially be used directly, or indirectly, by their children or students. It is recommended that applications and services transparently disclose the various methods that are legally available to provide parental consent and therefore enable parents and teachers to make an informed decision about which consent method is appropriate given the context in which the application or service is used.[144]

COMPLIANCE: CONSENT METHOD

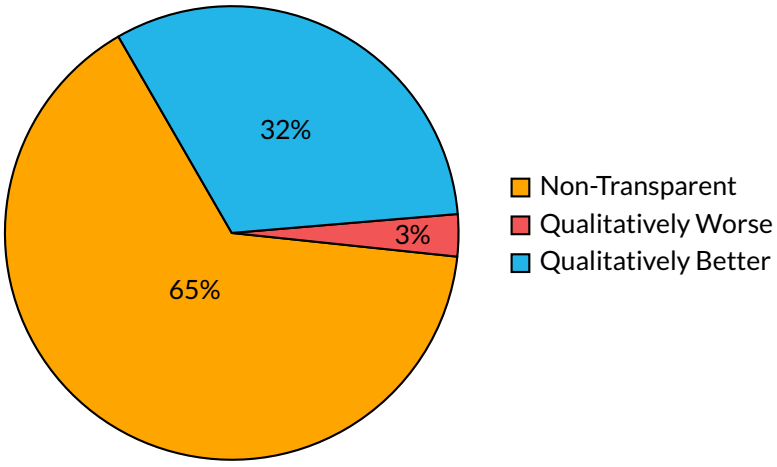


Figure 60: This chart illustrates the percentage of question responses about consent method. Qualitatively better question responses indicate the application or service discloses the methods available to provide verifiable parental consent. Qualitatively worse question responses indicate the application or service does not disclose the methods available to provide verifiable parental consent. Non-transparent responses indicate the terms are unclear about whether or not the application or service discloses the methods available to provide verifiable parental consent.

144 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(1)(2)(i)–(vi) (an operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent).

Additional Indicators

In addition to the concerns, our evaluation process identified additional indicators regarding third-party tracking and parental consent that further examine the intersection between parental consent and its implementation. These five questions are not primary indicators for the concerns themselves but rather are illustrative of additional tracking concerns and parental consent implementations that directly impact children, students, parents, teachers, and districts every day.

School Consent

Among the applications and services evaluated that require parental consent for the collection or disclosure of information from children or students, approximately 61 percent disclosed they placed this compliance obligation on the teacher, school, or district to obtain that verifiable parental consent. This disclosure is unexpected, because applications and services are still required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children under 13 years of age. However, there is an exception to the requirement that the application or service itself must obtain verifiable parental consent: A teacher, school, or district can otherwise provide consent on behalf of parents for the collection of personal information from their students under 13 years of age. However, this consent is limited to the educational context where the application or service is used and where students' information is collected solely for the use and benefit of the school or district.

From our analysis, we observed that the majority of applications and services that disclose parental consent is required are effectively shifting the compliance burden of obtaining that parental consent for students under 13 years of age to the teacher, school, or district. However, this practice is considered qualitatively worse in our evaluation process, because without contractual obligations in place to protect student information, it effectively exculpates these vendors from any parental-consent compliance obligations. By shifting the process of obtaining parental consent to the teacher, school or district, the application or service no longer needs to determine whether its users are children under the age of 13. Therefore, these applications and services can claim they have no actual knowledge that children under 13 are actually using their product and not disclose any mechanisms for parents to provide consent, as indicated in the Consent Method section.

This qualitatively worse practice of applications and services avoiding obtaining actual knowledge that users are under the age of 13 supports our previous findings in the Parental Consent section, wherein approximately 71 percent disclosed that parental consent is required under their terms or as stipulated under COPPA or FERPA. However, as indicated in the Consent Method section, we see that only approximately 32 percent disclosed a qualitatively better response of the actual methods available to provide verifiable parental consent. These findings further indicate applications and services where parental consent is required are more likely to be non-transparent about the methods in which to provide consent, ostensibly to avoid implementing technological methods for the consent-collection and -verification process, which places compliance burdens and penalties for non-compliance on teachers, schools, and districts.

AMONG SERVICES THAT REQUIRE PARENTAL CONSENT, PERCENT THAT PLACE OBLIGATION ON THE TEACHER, SCHOOL, OR DISTRICT TO OBTAIN PARENTAL CONSENT.

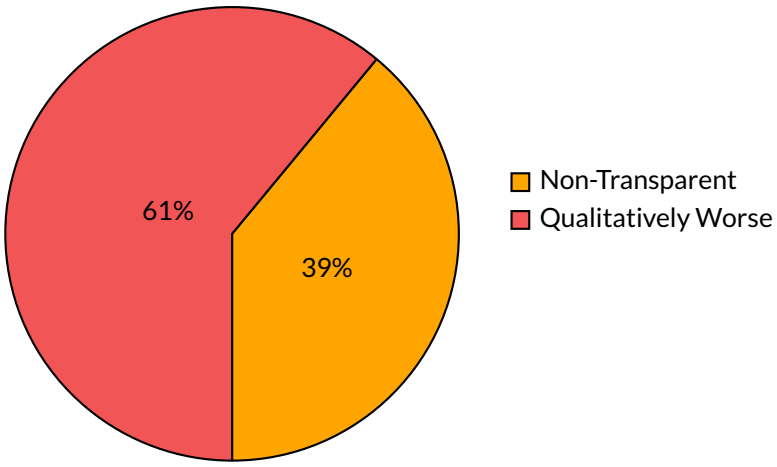


Figure 61: This chart illustrates the percentage of question responses about those services that require parental consent and how many transfer parental-consent obligations to the school or district. Qualitatively worse question responses indicate parental-consent obligations are transferred to the school or district. Non-transparent responses indicate the terms are unclear about whether or not the service transfers parental-consent obligations to the school or district.

Limit Consent

Among the applications and services evaluated and that require parental consent for the collection or disclosure of information from children or students, approximately only 16 percent disclosed that they limit consent to the collection and use of the child or student's personal information and do not automatically use that consent for the

disclosure of information to third parties. Accordingly, limiting parental consent to the collection of information is considered a qualitatively better practice in our evaluation process, because it removes improper pay-to-play incentives where in order to use an application or service, unequivocal parental consent must be given to disclose any collected information to third parties. This implied consent mechanism takes away parental-consent choice and agency on behalf of parents, teachers, and schools who are providing consent for their children and students under 13 years of age. Parents and teachers require meaningful choice about providing consent for the collection of information but not its unfettered use by third parties.

An application or service cannot condition a child's participation on sharing collected information with third parties beyond their trusted partners, affiliates, or service providers. Moreover, a parent is required to have the ability to consent to the collection and use of their child's personal information, without also consenting to the disclosure of that information to third parties.[145] However, approximately 83 percent of applications and services were non-transparent on this issue and, observationally, our findings indicate that parental consent is not properly bifurcated, because applications and services treat parental consent as a universal green light that any collected information can be be used as specified in their policies. This results in a lack of parental-consent notice and choice, where consent cannot be given without also giving consent to disclose that information to third parties. For example, our previous analysis found in the Data Shared section that approximately 90 percent of applications and services share personal information with third parties. In addition, our previous findings determined shared information is commonly used for third-party marketing, traditional advertising, and behavioral advertising. Therefore, given the common practice of applications and services disclosing child and student data to third parties for various purposes including marketing or advertising purposes, providing greater parental-consent notice and choice between the collection and disclosure of information will better protect children and students.

145 *See supra* note 92.

AMONG SERVICES THAT REQUIRE PARENTAL CONSENT, PERCENT THAT LIMIT CONSENT TO THE COLLECTION AND USE OF PERSONAL INFORMATION WITHOUT ALSO CONSENTING TO THE DISCLOSURE OF THE INFORMATION.

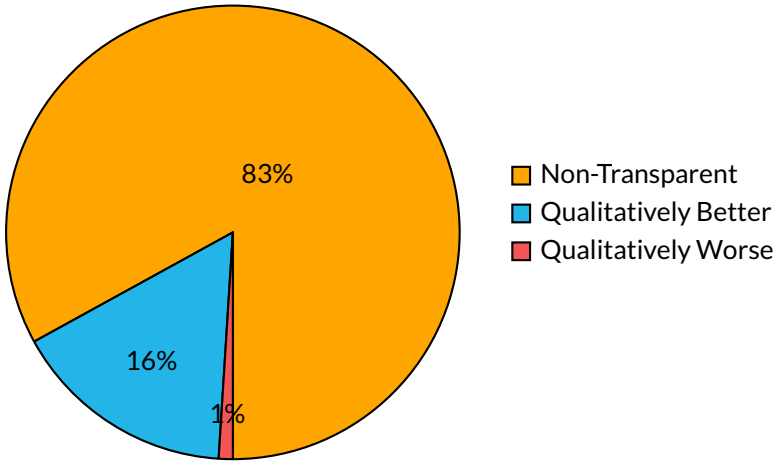


Figure 62: This chart illustrates the percentage of question responses about those services that require parental consent and how many allow for limitations with respect to third parties. Qualitatively better question responses indicate parental consent is limited with respect to third parties. Qualitatively worse question responses indicate parental consent is not limited with respect to third parties. Non-transparent responses indicate the terms are unclear about whether or not this service limits parental consent with respect to third parties.

Delete Data

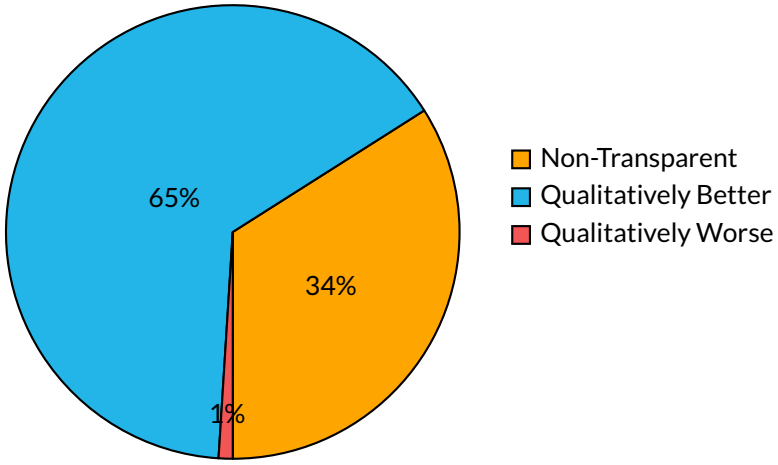
Among the applications and services evaluated that require parental consent for the collection or disclosure of information from children or students, approximately 65 percent disclosed they delete personal information from a child or student under 13 years of age if collected without parental consent. Accordingly, deleting child or student personal information if collected without parental consent is considered a qualitatively better practice in our evaluation process, because it is a requirement to remain in compliance with federal law.[146] This finding is expected given that approximately 71 percent of applications and services disclosed parental consent is required and therefore are predisposed to delete any child or student information collected if no parental consent is provided. This compliance practice is common to mitigate potential liability if the application or service manages the parental-consent process itself but more likely, as indicated in the School Consent section, to mitigate potential compliance

146 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(1) (if the operator has not obtained parental consent after a reasonable time from the date of the information collection, or been given actual notice that information from a child under the age of 13 has been collected without parental consent, the operator must delete the information from its records).

liability if teachers and schools are unable to produce verifiable records that parental consent was obtained on the vendor's behalf. However, the approximately 34 percent of non-transparent responses from applications and services about deleting information from children and students under 13 if collected without parental consent may be attributable to additional student data privacy agreements that exist privately between the vendor and schools or districts. These agreements define the parental-consent collection process on behalf of the schools or districts and the process of deleting collected information in the event parental consent is not obtained.

In addition, approximately 14 percent and 27 percent of applications and services disclosed that they are not intended for children or students respectively but also that they will delete any child or student data if provided to avoid potential liability. Therefore, applications and services that disclose parental consent is required, but are non-transparent about how child or student data is handled without verifiable consent, are likely to lose adoption among parents, teachers, schools, and districts — without additional student data privacy agreements in place — because of the increased risk for potential misuse and unauthorized disclosure of child and student information to third parties without proper consent.[147, 148]

AMONG SERVICES THAT REQUIRE PARENTAL CONSENT, PERCENT THAT DELETE PERSONAL INFORMATION IF COLLECTED WITHOUT PARENTAL CONSENT.



147 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.6(c) (an operator may terminate any service provided to a child whose parent has refused to permit the operator's further use or collection of the child's personal information or has directed the operator to delete the child's personal information).

148 *See supra* note 143.

Figure 63: This chart illustrates the percentage of question responses about those services that require parental consent and how many delete personal information if collected without parental consent. Qualitatively better question responses indicate children's personal information is deleted if collected without parental consent. Qualitatively worse question responses indicate children's personal information is not deleted if collected without parental consent. Non-transparent responses indicate the terms are unclear about whether or not this service deletes children's personal information if collected without parental consent.

School Official

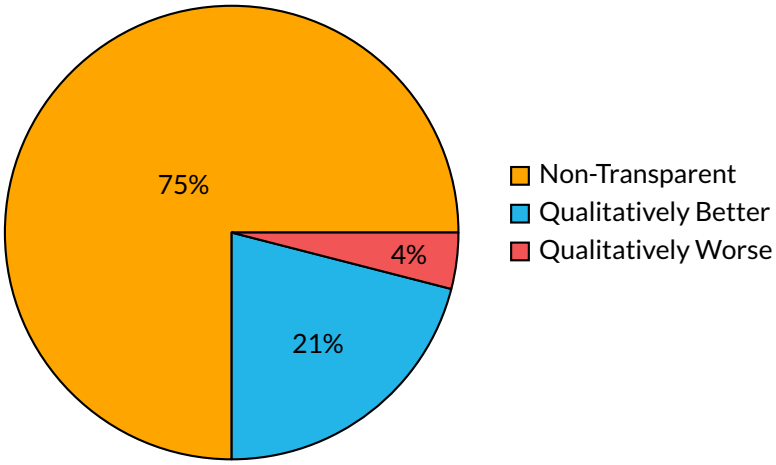
Among the applications and services evaluated that require parental consent for the collection or disclosure of information from children or students, approximately 21 percent disclosed they operate under the direct control of the educational institution and are designated a "School Official" under FERPA. Accordingly, schools must have written permission from the parent, or the eligible student over 18 years of age, in order to disclose any information from a student's education record. However, FERPA does allow schools and districts to disclose those records without consent under certain conditions, one of which includes disclosing a student's education records to applications and services designated a "School Official," if the operator is under the direct control of the education institution and information collected by the application or service is solely for the use and benefit of the school or district.

However, applications and services cannot simply disclose in their policies that they are a "School Official" and be properly designated as one. Schools and districts should enter into contractual relationships with applications and services that designate the vendor as a school official, which clearly defines the vendor's compliance obligations and places them under the direct control of the educational institution. These contractual agreements should also place additional requirements on the use of collected information for only educational purposes, as well as describing the process of obtaining parental consent. Approximately 75 percent of applications and services evaluated were non-transparent on this issue, although approximately 73 percent disclosed they are intended for students in the Students Intended section, and 57 percent disclosed they are intended for a school purpose, in which they are primarily designed, marketed, and used for preschool or K–12 school purposes.

Therefore, there is an apparent significant discrepancy between the percentage of applications and services that are non-transparent on this issue and the percentage of applications and services that provide products directly to students and schools. It is

recommended that these applications and services increase their transparency on this important issue and disclose in their policies that they may act as a "School Official," as specified in the school or district's annual FERPA notice, which describes how educational institutions can maintain direct control over applications and services in compliance with FERPA.[149] However, this disclosure also requires applications and services to include in their policies that they can enter into student data privacy agreements with educational institutions. Templates of student data privacy agreements should be made publicly available by the vendor so that teachers, schools, and districts can make informed decisions about whether or not to use an application or service that may become designated as a "School Official," based on the appropriate federal and state privacy and security protections provided in the agreement.[150, 151, 152, 153]

AMONG SERVICES THAT REQUIRE PARENTAL CONSENT, PERCENT THAT ARE UNDER THE DIRECT CONTROL OF THE EDUCATIONAL INSTITUTION AS A "SCHOOL OFFICIAL."



149 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.7(a) (an educational institution must annually notify parents of their rights to inspect and review a student's education records and make corrections, delete, or consent to the disclosure of information).

150 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(A) (an exception for disclosing personally identifiable information without obtaining parental consent exists for sharing with other school officials, including teachers within the same educational institution).

151 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(B) (an exception for disclosing personally identifiable information without obtaining parental consent exists for sharing data with a third party who is considered a "school official" with a legitimate educational interest and under direct control of the school for the use and maintenance of education records).

152 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii) (an educational institution must use reasonable methods to ensure that school officials use only information for which they have a legitimate educational interest).

153 California AB 1584 Privacy of Pupil Records, Cal. Ed. Code §49073.1(b)(8) (a local educational agency that enters into a contract with a third party must ensure the contract contains a description of how the local educational agency and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act [FERPA]).

Figure 64: This chart illustrates the percentage of question responses about those services that require parental consent and how many are designated as a "School Official." Qualitatively better question responses indicate the application or service is designated as a "School Official." Qualitatively worse question responses indicate the application or service is not designated as a "School Official." Non-transparent responses indicate the terms are unclear about whether or not the application or service is designated as a "School Official."

Do Not Track

Among the applications and services evaluated that disclosed they use third-party advertising services or tracking technologies to collect information, approximately 14 percent also disclosed they respond to a "do not track" signal or other opt-out mechanism. Accordingly, not disclosing how an application or service responds to web browser "do not track" signals or how users can opt out from advertising tracking is considered a qualitatively worse practice in our evaluation process, because it is a requirement to remain in compliance with various state laws.[154] This finding is based on the approximately 37 percent of applications and services as described in the Third-party Tracking section that disclosed qualitatively worse practices that they use third-party advertising or tracking technologies. Even with growing interest in tools for parents, teachers, and students to control how their data is collected, approximately 30 percent of applications and services that disclosed they use third-party tracking services do not also respond to any "do not track" signals. This finding is unexpected and likely attributable to industry confusion that because no standard "do not track" signal or tracking preference expression mechanism has been adopted by the World Wide Web Consortium (W3C), applications and services do not need to provide an ad hoc opt-out mechanism from a broad range of potential tracking services.[155] However, this industry confusion is likely responsible for the approximately 57 percent of applications and services that disclosed they use third-party tracking but are non-transparent about whether they respond to "do not track" signals or whether they provide any resources about an opt-out mechanism.[156]

---

154 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(5) (an operator is required to disclose how they respond to web browser "Do Not Track" signals or other mechanisms that provide consumers the ability to opt out of the collection of personally identifiable information about their online activities over time and across third-party websites).

155 World Wide Web Consortium, *Tracking Preference Expression (DNT)*, W3C Candidate Recommendation, (Oct. 19, 2017), https://www.w3.org/TR/tracking-dnt.

156 *See supra* note 52.

In general, regardless of whether or not applications or services disclose they use third-party tracking services, approximately 20 percent disclosed a qualitatively worse response that they do not respond to any "do not track" requests. Moreover, when examining only "do not track" disclosures, approximately 72 percent of applications and services are non-transparent about whether or not they respond to a "do not track" request. Given that the majority of applications and services are non-transparent on this issue, it is recommended that vendors provide more transparency about whether or not they respond to "do not track" signals, especially considering they already disclose they use third-party advertising services or tracking technologies to collect information from children and students. In addition, these applications and services should provide "do not track" controls that go beyond simply opting out users from receiving targeted advertisements but also should provide the ability to opt out from collection of other types of information such as behavioral data. However, this analysis lacks sufficient information in which to adequately determine "do not track" overall trends in the education industry, because approximately 42 percent of applications and services as described in the Third-Party Tracking section are non-transparent about whether or not they use third-party tracking services, and approximately 72 percent of applications and services are non-transparent about whether or not they respond to a "do not track" request.

Therefore, parents, teachers, schools, and districts need to exercise caution when evaluating whether to use popular edtech applications, and vendors need to provide greater transparency on this issue. Currently, the only way for consumers to obtain notice about whether an application or service uses third-party advertising trackers, if not disclosed in its policy, is to perform time-consuming observational assessments with third-party browser plug-ins or network traffic-monitoring tools. Increased transparency from applications and services about responding to "do not track" requests would increase parent and teacher choice in how children's and students' information is collected and provide more information by which to make an informed decision about whether or not to use a product.

AMONG SERVICES THAT DISCLOSE USE OF THIRD-PARTY TRACKING, PERCENT THAT DISCLOSE THEY RESPOND TO A "DO NOT TRACK" SIGNAL OR OTHER OPT-OUT MECHANISM.

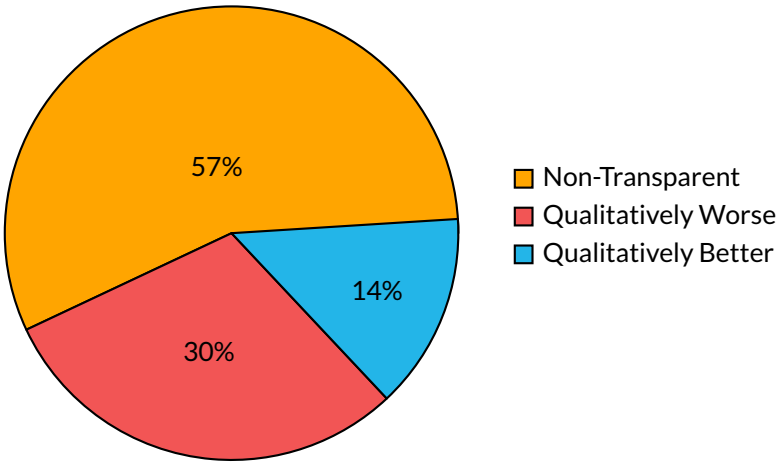


Figure 65: This chart illustrates the percentage of question responses about those services that disclose use of third-party tracking and how many respond to a "do not track" or other opt-opt mechanism. Qualitatively better question responses indicate the application or service responds to a "do not track" signal or other opt-out mechanism. Qualitatively worse question responses indicate the application or service does not respond to a "do not track" signal or other opt-out mechanism. Non-transparent responses indicate the terms are unclear about whether or not the application or service responds to a "do not track" signal or other opt-out mechanism.

APPENDIX A: NOT EXPECTED RESPONSES

In addition to our analyses, our evaluation process identified additional indicators regarding not-expected-to-be-disclosed responses to questions. Questions can be either expected- or not-expected-to-be disclosed given the intended use and context of the application or service. Not-expected responses are typically non-transparent, because the issues raised in the questions are not required to be disclosed in context, but analysis of not-expected non-transparent, qualitatively better, and qualitatively worse responses can still provide insight into how applications and services address issues in their policies when used in different scenarios.

Not Expected: Default Encryption

In addition to the analysis in the Default Encryption section, approximately 7 percent of not-expected observations indicated they still provide encryption of their application or service in the absence of collecting login information. Among this relatively 5 percent of not-expected-to-be-disclosed responses, approximately 100 percent observationally use encryption. Encrypting all data collected by an application or service is considered a qualitatively better practice in our evaluation process, because even if personal login information is not collected, non-personal information can still be intercepted if not encrypted and used in combination with other information for identification or exfiltration of sensitive data through unknown processes.

QUESTION: DEFAULT ENCRYPTION (NOT EXPECTED)

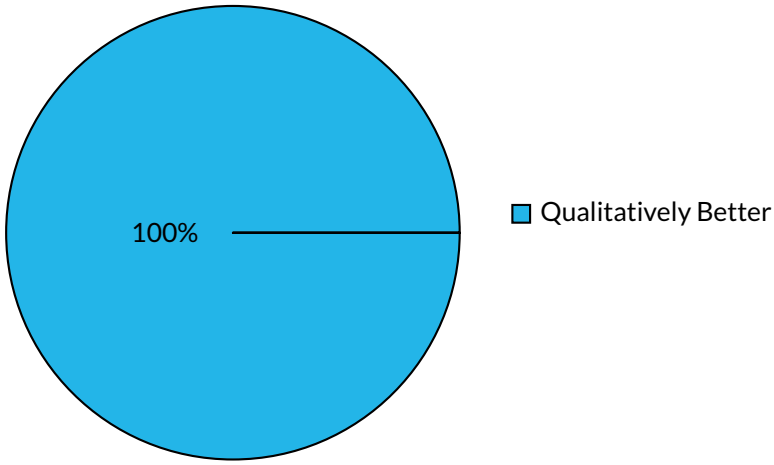


Figure 66: This chart illustrates the percentage of question responses about default encryption where the disclosure was not expected. Qualitatively better question responses indicate the application or service does use encryption.

Not Expected: Behavioral Advertising

In addition to the analysis in the Behavioral Advertising section, approximately 5 percent of applications and services were not expected to disclose a response in our evaluation process, because these applications and services did not disclose they were intended for children or students. However, these applications and services were still transparent about whether or not they display behavioral advertisements. Among the relatively 5 percent of not-expected-to-disclose responses, approximately 38 percent of applications and services disclosed they display behavioral advertisements, which is likely attributable to a small number of applications and services that are intended for children over 13, or students over 18 years of age. The approximately 25 percent of applications and services that disclosed they do not display behavioral advertisements, but otherwise did not disclose they are intended for children or students, is likely attributable to these services providing paid or subscription-based services rather than using advertising. In addition, these applications or services may simply be following industry best practices in the event children or students under 13 years of age were to use the service, even if they are not the intended audience.

QUESTION: BEHAVIORAL ADVERTISING (NOT EXPECTED)

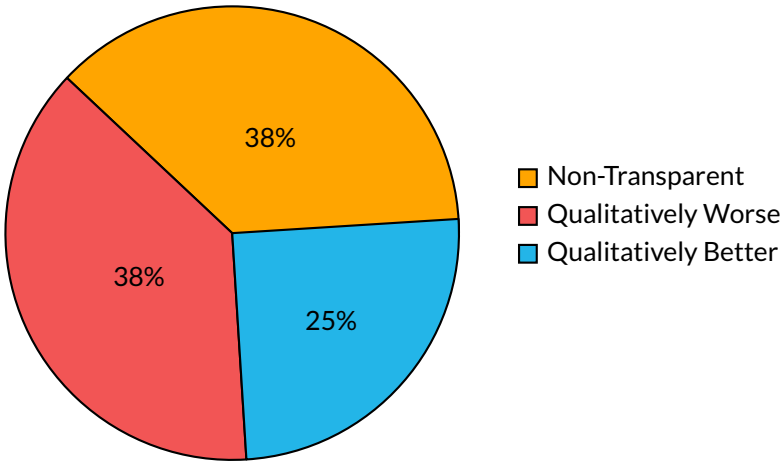


Figure 67: This chart illustrates the percentage of question responses about behavioral advertising where the disclosure was not expected. Qualitatively better question responses indicate the application or service does not display behavioral advertisements. Qualitatively worse question responses indicate the application or service does display behavioral

advertisements. Non-transparent responses indicate the terms are unclear about whether or not the application or service does display behavioral advertisements.

Not Expected: Visible Data

In addition to the analysis in the Visible Data section, approximately 10 percent of applications and services are not expected to disclose whether they allow personal information to be made publicly visible, because these applications and services did not disclose they were intended for children or students. Among the relatively 10 percent of not-expected-to-disclose responses, approximately 44 percent of applications and services disclosed qualitatively worse practices of making personal information publicly visible, likely because they target a general consumer audience, yet they are still commonly used with children and students under 13 years of age. Applications and services typically allow personal information to be made publicly available with features such as open text fields in profile settings, status updates, blog posts, forums, or other social interactions.

QUESTION: VISIBLE DATA (NOT EXPECTED)

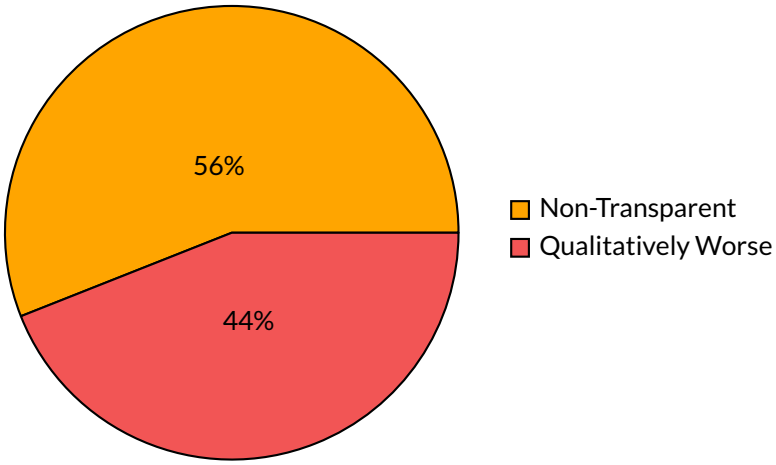


Figure 68: This chart illustrates the percentage of question responses about visible data where the disclosure was not expected. Qualitatively worse question responses indicate personal information can be displayed publicly. Non-transparent responses indicate the terms are unclear about whether or not personal information can be displayed publicly.

Not Expected: Collect PII

In addition to the analysis in the Collect PII section, approximately 6 percent of applications and services were not expected to disclose whether they collect personal information, because these applications and services did not disclose they were intended for children or students. Among the relatively 6 percent of not-expected responses, approximately 75 percent of applications and services disclosed they collect personal information, likely because they target a general consumer audience. However, collection of personal information in this scenario is still considered qualitatively worse in our evaluation process, because the application or service is commonly used by children and students under 13 years of age.

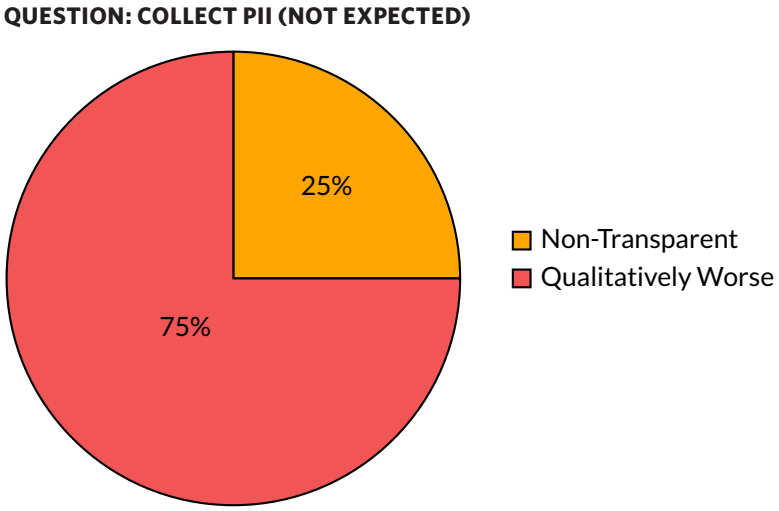


Figure 69: This chart illustrates the percentage of question responses about collecting PII where the disclosure was not expected. Qualitatively worse question responses indicate the application or service does collect personally identifiable information (PII). Non-transparent responses indicate the terms are unclear about whether or not the application or service collects personally identifiable information (PII).

Not Expected: Collection Limitation

In addition to the analysis in the Collection Limitation section, approximately 5 percent of applications and services were not expected to disclose, but did disclose, whether they limit the collection or use of information to data that are specifically required to use the application or service. Among this relatively 5 percent of not-expected responses, approximately 38 percent of applications and services disclose they limit the collection of information, which is a qualitatively better practice given their use by children and

students. This practice of not-expected collection limitation mitigates the otherwise high percentage of not-expected collection of personal information in the Collect PII section, where applications and services assume they only target a general consumer audience yet are still commonly used with children and students under 13 years of age.

PRIVACY: COLLECTION LIMITATION (NOT EXPECTED)

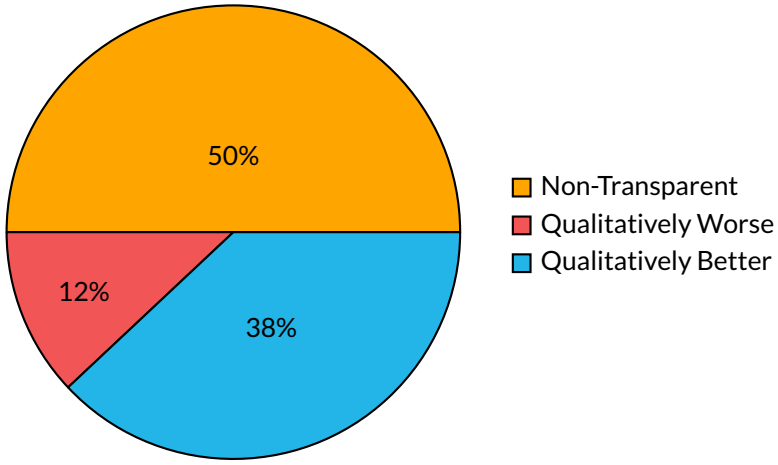


Figure 70: This chart illustrates the percentage of question responses about collection limitation where the disclosure was not expected. Qualitatively better question responses indicate the application or service limits the collection or use of information to data that are specifically required to use the application or service. Qualitatively worse question responses indicate the application or service does not limit the collection or use of information to data that are specifically required to use the application or service. Non-transparent responses indicate the terms are unclear about whether or not the application or service limits the collection or use of information to data that are specifically required to use the application or service.

Not Expected: Purpose Limitation

In addition to the analysis in the Purpose Limitation section, approximately 5 percent of applications and services were not expected to disclose whether they limit their use of information to the purpose for which it was collected, because they disclosed that the service is not primarily directed or targeted to children or students under 13 years of age. However, among the relatively 5 percent of not-expected responses, approximately 62 percent disclosed qualitatively better practices. These not-expected qualitatively better disclosures are likely attributable to vendors including industry best practices in their policies in the event the application or service is ever used by children or students. This type of not-expected disclosure is considered a qualitatively better practice in

our evaluation process, because more and more consumer products are not primarily intended or directed to children or students under 13 years of age but are commonly being used by children under 13 at home and with students in school, even if they are not the intended audience.

QUESTION: PURPOSE LIMITATION (NOT EXPECTED)

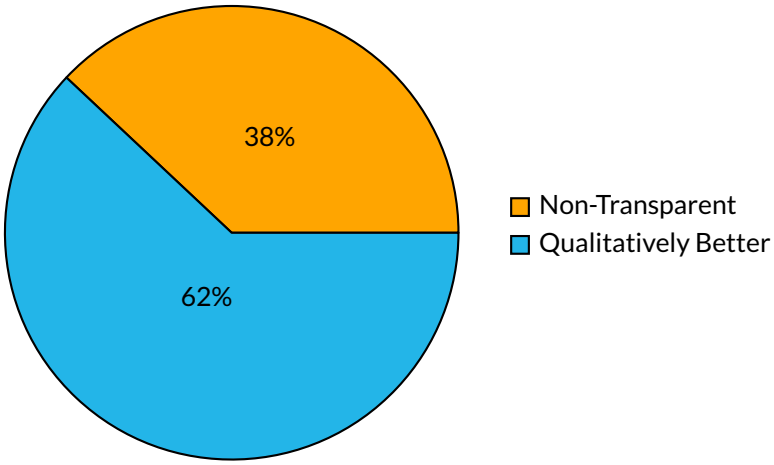


Figure 71: This chart illustrates the percentage of question responses about purpose limitation where the disclosure was not expected. Qualitatively better question responses indicate the application or service does limit the use of data collected to the educational purpose for which it was collected. Non-transparent responses indicate the terms are unclear about whether or not the application or service limits the use of data collected to the educational purpose for which it was collected.

Not Expected: Transit Encryption

In addition to the analysis in the Transit Encryption section, approximately 57 percent of applications and services were not expected to disclose responses in our evaluation process, because they did not disclose they were intended for students or children under 13 years of age but still indicated whether they encrypt information while in transit. The distinction between expected and not-expected qualitatively better disclosures relates to whether state data breach- or encryption-related laws apply in context. Among the relatively 57 percent of not-expected responses, approximately 31 percent of applications and services disclosed that collected information is encrypted while in transit. This high percentage of not-expected qualitatively better disclosures is consistent with our findings in the Children Intended and Students Intended sections, where approximately 14 percent and 27 percent respectively of applications and services

disclosed they are not intended for students or children under 13 years of age but still disclosed they use reasonable security standards of encrypting information in transit, likely because as a general audience service they collect more personal information or follow industry best practices of encrypting data.

SECURITY: TRANSIT ENCRYPTION (NOT EXPECTED)

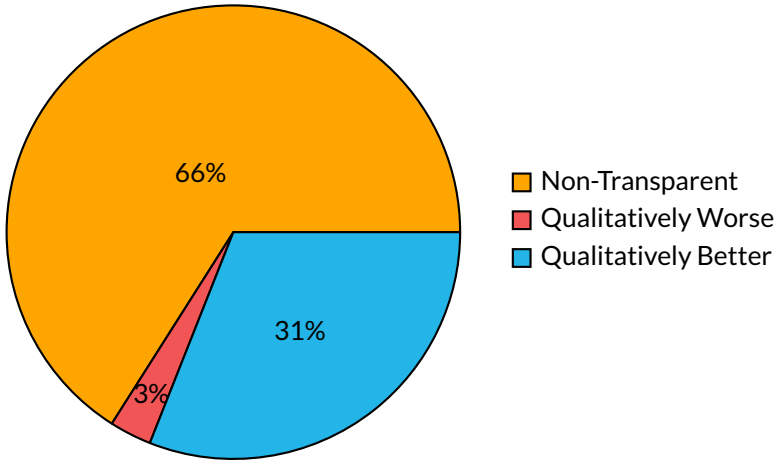


Figure 72: This chart illustrates the percentage of question responses about transit encryption wherein the disclosure was not expected. Qualitatively better question responses indicate collected information is encrypted while in transit. Qualitatively worse question responses indicate collected information is not encrypted while in transit. Non-transparent responses indicate the terms are unclear about whether or not collected information is encrypted while in transit.

Not Expected: Storage Encryption

In addition to the analysis in the Storage Encryption section, approximately 54 percent of applications and services were not expected to disclose that they encrypt information while in storage. The distinction between expected and not-expected qualitatively better disclosures relates to whether state data breach- or encryption-related laws apply in context. Among the relatively 54 percent of not expected responses, approximately 17 percent of applications and services disclosed that collected information is encrypted while in storage. The high not-expected-to-disclose non-transparent responses to this issue are likely attributable to applications and services only referencing use of expected reasonable security standards, which include encryption of collected information while in storage. The majority of applications and services evaluated disclosed that they provide reasonable security practices but do not prescriptively disclose that they provide the reasonable security practice of encrypting collected information while it is stored. In contrast, compared to the not-expected responses in

the Transit Encryption section, an approximately not-expected 14 percent greater percentage of applications and services disclosed that collected information is encrypted while it is in transit than while it is in storage.

QUESTION: STORAGE ENCRYPTION (NOT EXPECTED)

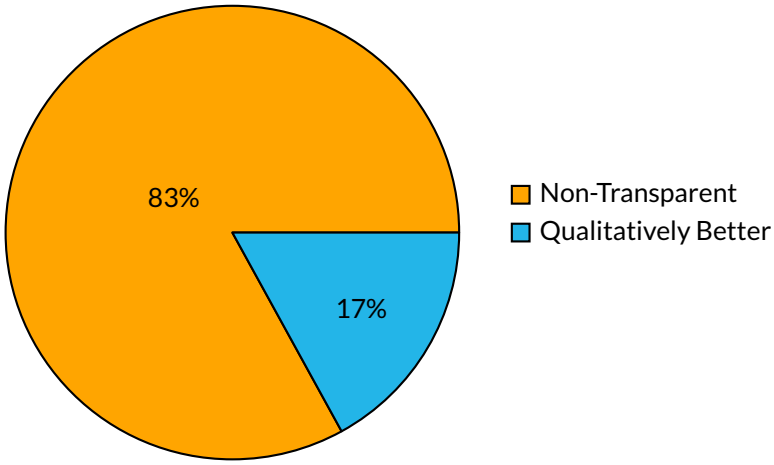


Figure 73: This chart illustrates the percentage of question responses about storage encryption wherein the disclosure was not expected. Qualitatively better question responses indicate collected information is encrypted while in storage. Non-transparent responses indicate the terms are unclear about whether or not collected information is encrypted while in storage.

Not Expected: Breach Notice

In addition to the analysis in the Breach Notice section, approximately 18 percent of applications and services were not expected to disclose responses in our evaluation process, because they did not disclose they were intended for students or children under 13 years of age but still indicated whether notice would be provided to affected users if their unencrypted collected information is disclosed to unauthorized individuals in a data breach. Among the relatively 18 percent of not-expected responses, approximately 15 percent of applications and services disclosed they provide notice in the event of a data breach, which is likely attributable to a small number of services that collect little or no personal information as indicated in the Collect PII section but still provide data breach notifications to affected users, which is considered an industry best practice.

SECURITY: BREACH NOTICE (NOT EXPECTED)

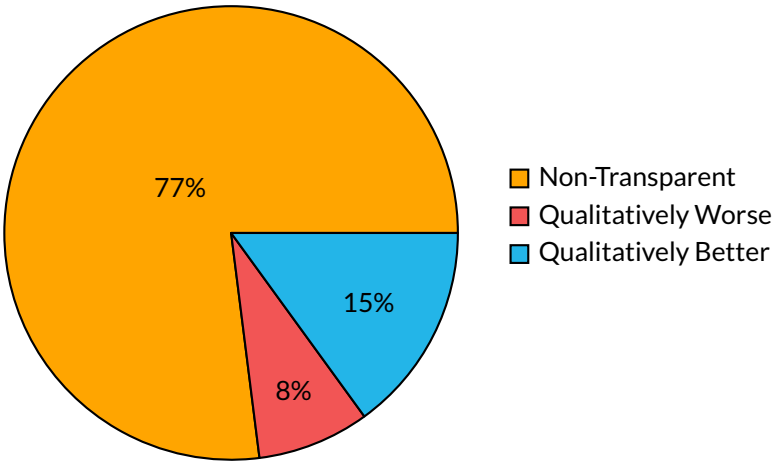


Figure 74: This chart illustrates the percentage of question responses about breach notice wherein the disclosure was not expected. Qualitatively better question responses indicate notice is provided to affected users if their unencrypted collected information is disclosed to unauthorized individuals in a data breach. Qualitatively worse question responses indicate no notice is provided to affected users if their unencrypted collected information is disclosed to unauthorized individuals in a data breach. Non-transparent responses indicate the terms are unclear about whether or not notice is provided to affected users if their unencrypted collected information is disclosed to unauthorized individuals in a data breach.

APPENDIX B: EVALUATION QUESTIONS

The questions we use in our privacy evaluations are organized by the Fair Information Practice Principles (FIPPs). These principles form the basis for national and international privacy regulations, guidelines, and best practice.[157]

Observation

Policy Available: Are the policies for the specific service available (and not, for example, for the public-facing website)?

Same Policy: Do Android or iOS app privacy policies link to the same privacy policy URL location as the home page policy?

Default Encryption: Do the homepage, login page, or pages accessed while logged in use encryption with HTTPS?

Encryption Required: Do the homepage, login page, or pages accessed while logged in force encryption back to HTTPS if changed to HTTP?

Use Trackers: Does the application or service use trackers on its homepage, registration page, or while a user is logged-in?

Policy Available

Policy Links: Are hyperlinks to the vendor's policies available on the homepage and labeled Privacy Policy or Terms of Use?

Policy Accessible: Are the policies available in a human and machine readable format that is accessible on the web, mobile devices, screen readers or assistive technologies?

Allow Crawling: Do the policies allow machine crawling or indexing?

Policy Purchase: Are the policies available on all product purchase or acquisition webpages?

Policy Registration: Are the policies available on a new account registration webpage for review prior to a user creating a new account with the service or application?

---

157 *See supra* note 9; Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Account Type

Free Account: Can you create a free sample account with the application or service?

Access Code: Does the application or service require the purchase of hardware or a School access code to create an account?

Purchase Options: Does the application or service offer a separate paid version or In-App-Purchases?

Policy Errors

Policy Readability: Do the policies contain structural or typographical errors?

Transparency

Effective Date: Do the policies clearly indicate the version or effective date of the policies?

Change Log: Do the policies clearly indicate a changelog or past versions of the policies are available for review?

Services Include: Do the policies clearly indicate the websites, services, or mobile applications that are covered by the policies?

Review Changes: Do the policies clearly indicate whether or not any updates or material changes to the policies will be accessible for review by a user prior to the new changes being effective?

Effective Changes: Do the policies clearly indicate whether or not any updates or material changes to the policies are effective immediately and continued use of the application or service indicates consent?

Change Notice: Do the policies clearly indicate whether or not a user is notified if there are any material changes to the policies?

Method Notice: Do the policies clearly indicate the method used to notify a user when policies are updated or materially change?

Cookie Notice: Do the policies clearly indicate the vendor provides prominent notice on the homepage that the website or service uses cookies?

Vendor Contact: Do the policies clearly indicate whether or not a user can contact the vendor about any privacy policy questions, complaints, or material changes to the policies?

Quick Reference: Do the policies clearly indicate short explanations, layered notices, a table of contents, or privacy principles of the vendor?

Preferred Language: Do the policies clearly indicate they are available in a language other than English?

Children Intended: Do the policies clearly indicate whether or not the service is intended to be used by children under the age of 13?

Teens Intended: Do the policies clearly indicate whether or not the service is intended to be used by teens 13 to 18 years of age?

Adults Intended: Do the policies clearly indicate whether or not the service is intended to be used by adults over the age of 18?

Parents Intended: Do the policies clearly indicate whether or not the service is intended to be used by parents or guardians?

Students Intended: Do the policies clearly indicate whether or not the service is intended to be used by students in preschool or K-12?

Teachers Intended: Do the policies clearly indicate whether or not the service is intended to be used by teachers?

Focused Collection

Collect PII: Do the policies clearly indicate whether or not the vendor collects Personally Identifiable Information (PII)?

PII Categories: Do the policies clearly indicate what categories of Personally Identifiable Information are collected by the application or service?

Geolocation Data: Do the policies clearly indicate whether or not geolocation data are collected?

Health Data: Do the policies clearly indicate whether or not any biometric data are collected?

Behavioral Data: Do the policies clearly indicate whether or not any behavioral data are collected?

Sensitive Data: Do the policies clearly indicate whether or not sensitive personal information is collected?

Usage Data: Do the policies clearly indicate whether or not the application or service collects non-personal information such as a user's persistent identifier, unique device ID, IP address, or other device information?

Lunch Status: Do the policies clearly indicate whether or not the vendor collects information on free or reduced lunch status?

Student Data: Do the policies clearly indicate whether or not the vendor collects personal information or education records from preK-12 students?

Child Data: Do the policies clearly indicate whether or not the vendor collects personal information online from children under 13 years of age?

Data Excluded: Do the policies clearly indicate whether or not the vendor does not collect specific types of data?

Coverage Excluded: Do the policies clearly indicate whether or not the vendor excludes specific types of collected data from coverage under its privacy policy?

Collection Limitation: Do the policies clearly indicate whether or not the vendor limits the collection or use of information to only data that are specifically required for the application or service?

Data Sharing

Data Shared: Do the policies clearly indicate if collected information (this includes data collected via automated tracking or usage analytics) is shared with third parties?

Data Categories: Do the policies clearly indicate what categories of information are shared with third parties?

Sharing Purpose: Do the policies clearly indicate the vendor's intention or purpose for sharing a user's personal information with third parties?

Third-Party Analytics: Do the policies clearly indicate whether or not collected information is shared with third parties for analytics and tracking purposes?

Third-party Research: Do the policies clearly indicate whether or not collected information is shared with third parties for research or product improvement purposes?

Third-party Marketing: Do the policies clearly indicate whether or not personal information is shared with third parties for advertising or marketing purposes?

Exclude Sharing: Do the policies clearly indicate whether the vendor specifies the categories of information that will not be shared with third parties?

Data Sold: Do the policies clearly indicate whether or not a user's personal information is sold or rented to third parties?

Data Acquired: Do the policies clearly indicate whether or not a user's information is acquired from a third-party by the vendor?

Data Deidentified: Do the policies clearly indicate whether or not a user's information that is shared or sold to a third-party is only done so in an anonymous or de-identified format?

Deidentified Process: Do the policies clearly indicate whether or not a user's personal information is de-identified with a reasonable level of justified confidence, or the vendor provides links to any information that describes their de-identification process?

Outbound Links: Do the policies clearly indicate whether or not outbound links on the site to third-party external websites are age appropriate?

Authorized Access: Do the policies clearly indicate whether or not a third party is authorized to access a user's information?

Third-Party Collection: Do the policies clearly indicate whether or not a user's personal information is collected by a third party?

Data Misuse: Do the policies clearly indicate whether or not a user's information can be deleted from a third party by the vendor, if found to be misused by the third party?

Third-Party Providers: Do the policies clearly indicate whether or not third-party services are used to support the internal operations of the vendor's application or service?

Third-Party Roles: Do the policies clearly indicate the role of third-party service providers?

Third-party Categories: Do the policies clearly indicate the categories of third parties, subsidiaries, or affiliates with whom the vendor shares data?

Third-Party Policy: Do the policies clearly indicate whether a link to a third-party service provider, data processor, partner, or affiliate's privacy policy is available for review?

Vendor Combination: Do the policies clearly indicate whether or not data collected or maintained by the **vendor** can be augmented, extended, or combined with data from third party sources?

Third-Party Combination: Do the policies clearly indicate whether or not data shared with third parties can be augmented, extended, or combined with data from additional third party sources?

Social Login: Do the policies clearly indicate whether or not social or federated login is supported to use the service?

Social Collection: Do the policies clearly indicate whether or not the vendor collects information from social or federated login providers?

Social Sharing: Do the policies clearly indicate whether or not the vendor shares information with social or federated login providers?

Third-Party Limits: Do the policies clearly indicate whether or not third parties have contractual limits on how they can use personal information that is shared or sold to them?

Combination Limits: : Do the policies clearly indicate whether or not third parties have contractual limits that prohibit re-identification or combining data with other data sources that are shared or sold to them?

Respect for Context

Purpose Limitation: Do the policies clearly indicate whether or not the vendor limits the use of data collected by the application to the educational purpose for which it was collected?

Data Purpose: Do the policies clearly indicate the context or purpose in which data are collected?

Data Type: Do the policies clearly indicate specific types of personal information (PII, Non-PII, Children's PII, Sensitive information, etc.)?

Account Type: Do the policies clearly indicate different types or classes of user accounts?

Combination Type: Do the policies clearly indicate whether or not Personally Identifiable Information (PII) combined with non-PII would be treated as PII?

Context Notice: Do the policies clearly indicate whether or not notice is provided to a user if the vendor changes the context in which data are collected?

Practice Changes: Do the policies clearly indicate whether or not the vendor will obtain consent if the practices in which data are collected change or are inconsistent with contractual requirements?

Community Guidelines: Do the policies clearly indicate whether or not the vendor may terminate a user's account if they engage in any prohibited activities?

Individual Control

User Submission: Do the policies clearly indicate whether or not a user can create or upload content to the service?

Content Control: Do the policies clearly indicate whether or not a user's content is stored with the vendor or a third party?

Collection Consent: Do the policies clearly indicate whether or not the vendor requests opt-in consent from a user at the time information is collected?

Restriction Notice: Do the policies clearly indicate whether or not the vendor is able to restrict or remove a user's content without notice or consent?

User Control: Do the policies clearly indicate whether or not a user can control the vendor or third party's use of their information through privacy settings?

Opt-Out Consent: Do the policies clearly indicate whether or not a user can provide consent or opt-out from disclosure of their data to a third party?

Disclosure Request: Do the policies clearly indicate whether or not a user can request the vendor to disclose all the personal information or records collected about them or shared with third parties?

Disclosure Notice: Do the policies clearly indicate whether or not in the event a vendor discloses information in response to a government or legal request, if they will contact the affected user, school, parent, or student with notice of the request, so they may choose to seek a protective order or other legal remedy?

Data Ownership: Do the policies clearly indicate whether or not a student, educator, parent, or the school retains ownership to the Intellectual Property rights of the data collected or uploaded to the application or service?

Copyright License: Do the policies clearly indicate whether or not the vendor may claim a copyright license to the data or content collected from a user?

Copyright Limits: Do the policies clearly indicate whether or not the vendor may limit its copyright license of a user's data?

Copyright Violation: Do the policies clearly indicate whether or not the vendor provides notice to a user if their content is removed or disabled because of a claim it violates the Intellectual Property rights of others?

Access and Accuracy

Access Data: Do the policies clearly indicate whether or not the vendor provides a method to access and review a user's personal information for authorized individuals?

Restrict Access: Do the policies clearly indicate whether or not the vendor may restrict access for unauthorized individuals to a user's data?

Review Data: Do the policies clearly indicate whether or not there is a process available for the school, parents, or eligible students to review student information?

Maintain Accuracy: Do the policies clearly indicate whether or not the vendor takes steps to maintain the accuracy of data they collect and store?

Data Modification: Do the policies clearly indicate whether or not the vendor provides the ability to modify a user's inaccurate data for authorized individuals?

Modification Process: Do the policies clearly indicate whether or not there is a process for the school, parents, or eligible students to modify inaccurate student information?

Modification Request: Do the policies clearly indicate whether or not the school, parents, or eligible students may submit a request to the vendor to modify a student's inaccurate personal information?

Modification Notice: Do the policies clearly indicate how long the vendor has to modify a user's inaccurate data after given notice?

Retention Policy: Do the policies clearly indicate the vendor's data retention policy, including any data sunsets or any time-period after which a user's data will be automatically deleted if they are inactive on the application or service?

Retention Limits: Do the policies clearly indicate whether or not the vendor will limit the retention of a user's data unless a valid request to inspect data are made?

Deletion Purpose: Do the policies clearly indicate whether or not the vendor will delete a user's personal information when the data are no longer necessary to complete the purpose for which it was collected?

Account Deletion: Do the policies clearly indicate whether or not a user's data are deleted upon account cancellation or termination?

User Deletion: Do the policies clearly indicate whether or not a user can delete all of their personal and non-personal information from the vendor?

Deletion Process: Do the policies clearly indicate whether or not there is a process for the school, parent, or eligible student to delete a student's personal information?

Deletion Notice: Do the policies clearly indicate how long the vendor may take to delete a user's data after given notice?

User Export: Do the policies clearly indicate whether or not a user can export or download their data, including any user created content on the application or service?

Legacy Contact: Do the policies clearly indicate whether or not a user may assign an authorized account manager or legacy contact to access and download their data in the event the account becomes inactive?

Data Transfer

Transfer Data: Do the policies clearly indicate whether or not a user's data can be transferred by the vendor in the event of a merger, acquisition, or bankruptcy?

Data Assignment: Do the policies clearly indicate whether or not the vendor can assign its rights or delegate its duties under the policies to a third party without notice or consent?

Transfer Notice: Do the policies clearly indicate whether or not a user will be notified and allowed to provide consent to a data transfer to a third-party successor, in the event of a vendor bankruptcy, merger, or acquisition?

Delete Transfer: Do the policies clearly indicate whether or not a user can request to delete their data prior to its transfer to a third-party successor in the event of a vendor bankruptcy, merger, or acquisition?

Contractual Limits: Do the policies clearly indicate whether or not the third-party successor of a data transfer is contractually required to provide the same level of privacy protections as the vendor?

Security

Verify Identity: Do the policies clearly indicate whether or not a user's identity is verified with personal information collected by the vendor or third party?

Account Required: Do the policies clearly indicate whether or not the vendor requires a user to create an account with a username and password in order to use the Service?

Managed Account: Do the policies clearly indicate whether or not the vendor provides user managed accounts for a parent, teacher, school or district?

Two-Factor Protection: Do the policies clearly indicate whether or not the security of a user's account is protected by two-factor authentication?

Security Agreement: Do the policies clearly indicate whether or not a third party with access to a user's information is contractually required to provide the same level of security protections as the vendor?

Reasonable Security: Do the policies clearly indicate whether or not reasonable security standards are used to protect the confidentiality of a user's personal information?

Employee Access: Do the policies clearly indicate whether or not the vendor implements physical access controls or limits employee access to user information?

Transit Encryption: Do the policies clearly indicate whether or not all data in transit is encrypted?

Storage Encryption: Do the policies clearly indicate whether or not all data at rest is encrypted?

Data Control: Do the policies clearly indicate whether or not personal information are stored outside the direct control of the vendor?

Breach Notice: Do the policies clearly indicate whether or not the vendor provides notice in the event of a data breach to affected individuals?

Responsible Use

Safe Interactions: Do the policies clearly indicate whether or not a user can interact with other users, or students can interact with other students in the same classroom, or school?

Unsafe Interactions: Do the policies clearly indicate whether or not a user can interact with strangers, including adults?

Share Profile: Do the policies clearly indicate whether or not information must be shared or revealed by a user in order to participate in social interactions?

Visible Data: Do the policies clearly indicate whether or not a user's personal information can be displayed publicly in any way?

Profile Visibility: Do the policies clearly indicate whether or not a user's personal information can be displayed publicly, outside the context of social interactions?

Control Visibility: Do the policies clearly indicate whether or not a user has control over how their personal information is displayed to others?

Block Content: Do the policies clearly indicate whether or not an educator, parent, or a school has the ability to filter or block inappropriate content, or social interactions with unauthorized individuals?

Report Abuse: Do the policies clearly indicate whether or not a user can report abuse or cyber-bullying?

Monitor Content: Do the policies clearly indicate whether or not user content is reviewed, screened, or monitored by the vendor?

Filter Content: Do the policies clearly indicate whether or not the vendor takes reasonable measures to delete all personal information from a user's postings before they are made publicly visible?

Moderate Interactions: Do the policies clearly indicate whether or not social interactions between users on the website or application are moderated?

Log Interactions: Do the policies clearly indicate whether or not social interactions are logged by the vendor?

School Audit: Do the policies clearly indicate whether or not social interactions may be audited by a school or district?

Parent Audit: Do the policies clearly indicate whether or not social interactions may be audited by a parent or guardian?

User Audit: Do the policies clearly indicate whether or not social interactions may be audited by a user or eligible student?

Safe Tools: Do the policies clearly indicate whether or not tools and processes that support safe and appropriate social interactions on the application or service are provided by the vendor?

Advertising

Service Messages: Do the policies clearly indicate whether or not a user will receive service or administrative related email or text message communications from the vendor or third party?

Traditional Ads: Do the policies clearly indicate whether or not traditional advertisements are displayed to a user based on webpage content, but not a user's data?

Behavioral Ads: Do the policies clearly indicate whether or not behavioral or contextual advertising based on a student's personal information are displayed?

Third-Party Tracking: Do the policies clearly indicate whether or not third-party advertising services or tracking technologies collect any information from a user of the application or service?

Track Users: Do the policies clearly indicate whether or not a user's information is used to track and target advertisements on other third-party websites or services?

Ad Profile: Do the policies clearly indicate whether or not the vendor allows third parties to use a student's data to create a profile, engage in data enhancement, social advertising, or target advertising to students, parents, teachers, or the school?

Child Ads: Do the policies clearly indicate whether or not advertisements are displayed to children under 13 years of age?

Filter Ads: Do the policies clearly indicate whether or not advertisements that are age inappropriate for minors are filtered (e.g., alcohol, gambling, violent, or sexual content)?

Marketing Messages: Do the policies clearly indicate whether or not the vendor may send marketing emails, text messages, or other related communications that may be of interest to a user?

Third-Party Promotions: Do the policies clearly indicate whether or not the vendor allows a user to participate in any sweepstakes, contests, surveys, or other similar promotions?

Unsubscribe Ads: Do the policies clearly indicate whether or not a user can opt-out of traditional, contextual, or behavioral advertising?

Unsubscribe Marketing: Do the policies clearly indicate whether or not a user can opt-out or unsubscribe from a vendor or third party marketing communication?

DoNotTrack Response: Do the policies clearly indicate whether or not the vendor responds to a "Do Not Track" signal or other opt-out mechanisms from a user?

DoNotTrack Description: Do the policies clearly indicate whether the vendor provides a hyperlink to a description, including the effects, of any program or protocol the vendor follows that offers consumers a choice not to be tracked?

Compliance

Actual Knowledge: Do the policies clearly indicate whether or not the vendor has actual knowledge that personal information from children under 13 years of age is collected by the application or service?

Child Audience: Do the policies clearly indicate whether or not the application or service is directed to children under 13, or (even if for an older audience) would the service appeal to children under 13 years of age?

COPPA Notice: Do the policies clearly indicate whether or not the vendor describes: (1) what information is collected from children under 13 years of age, (2) how that information is used, and (3) its disclosure practices of that information?

COPPA Offline: Do the policies clearly indicate whether or not the vendor collects personal information from children under 13 years of age "offline"?

Restrict Account: Do the policies clearly indicate whether or not the vendor restricts creating an account for a child under 13 years of age?

Restrict Purchase: Do the policies clearly indicate whether or not the vendor restricts in-app purchases for a child under 13 years of age?

Safe Harbor: DDo the policies clearly indicate whether or not the application or service participates in an FTC approved COPPA safe harbor program?

Teen Data: Do the policies clearly indicate whether or not personal information from teens 13 to 18 years of age are collected?

School Purpose: Do the policies clearly indicate whether or not the application or service is primarily used for preschool or K-12 school purposes and was designed and marketed for preschool or K-12 school purposes?

Education Records: Do the policies clearly indicate the process by which education records are entered into the application or service? For example, are data entered by district staff, school employees, parents, teachers, students, or some other person?

FERPA Notice: Do the policies clearly indicate whether or not the vendor provides a separate agreement that provides notice to users of their rights, under FERPA?

School Official: Do the policies clearly indicate whether or not the vendor is under the direct control of the educational institution and designated a 'school official,' under FERPA?

Directory Information: Do the policies clearly indicate whether or not the vendor discloses student information as 'Directory Information' under a FERPA exception?

Parental Consent: Do the policies clearly indicate whether or not 'verifiable parental consent' should be obtained before they collect or disclose personal information?

Limit Consent: Do the policies clearly indicate whether or not a parent can consent to the collection and use of their child's personal information without also consenting to the disclosure of the information to third parties?

Withdraw Consent: Do the policies clearly indicate whether or not the vendor responds to a request from a parent or guardian to prevent further collection of their child's information?

Delete Child: Do the policies clearly indicate whether or not the vendor deletes personal information from a student or child under 13 years of age if collected without parental consent?

Consent Method: Do the policies clearly indicate whether or not the vendor provides direct notice to parents of its collection and disclosure practices with method to provide verifiable parental consent, under COPPA?

Internal Operations: Do the policies clearly indicate whether or not the vendor can collect and use personal information from children without parental consent to support the 'internal operations' of the vendor's website or service?

COPPA Exception: Do the policies clearly indicate whether or not the vendor collects personal information from children without verifiable parental consent for the sole purpose of trying to obtain consent under COPPA?

FERPA Exception: Do the policies clearly indicate whether or not the vendor may disclose personal information without verifiable parental consent under a FERPA exception?

School Consent: Do the policies clearly indicate whether or not responsibility or liability for obtaining verified parental consent is transferred to the school or district?

Policy Jurisdiction: Do the policies clearly indicate the vendor's jurisdiction that applies to the construction, interpretation, and enforcement of the policies?

Dispute Resolution: Do the policies clearly indicate whether or not the vendor requires a user to waive the right to a jury trial, or settle any disputes by Alternative Dispute Resolution (ADR)?

Class Waiver: Do the policies clearly indicate whether or not the vendor requires waiver of any rights to join a class action lawsuit?

Law Enforcement: Do the policies clearly indicate whether or not the vendor can use or disclose a user's data under a requirement of applicable law, to comply with a legal process, respond to governmental requests, enforce their own policies, for assistance in fraud detection and prevention, or to protect the rights, privacy, safety or property of the vendor, its users, or others?

Privacy Award: Do the policies clearly indicate whether or not the vendor has signed any privacy pledges or received any other privacy certifications?

GDPR Transfer: Do the policies clearly indicate whether or not a user's data are subject to International data jurisdiction laws, such as a privacy shield, or a safe harbor framework that protects the cross-border transfer of a user's data?

GDPR Contact: Do the policies clearly indicate whether or not the vendor provides a Data Protection Officer (DPO) or other contact to ensure GDPR compliance?

Accountability Audit: Do the policies clearly indicate whether or not the data privacy or security practices of the vendor are internally or externally audited to ensure compliance?

ABOUT COMMON SENSE

Common Sense is a nonprofit, nonpartisan organization dedicated to improving the lives of kids, families, and educators by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology. Our independent research is designed to provide parents, educators, health organizations, and policymakers with reliable, independent data on children's and student's use of media and technology and the impact it has on their physical, emotional, social, and intellectual development.

For more information, visit **commonsense.org/education/privacy**.

For inquiries, contact **privacy@commonsense.org**.

OUR OFFICES

San Francisco Headquarters
650 Townsend Street, Suite 435
San Francisco, CA 94103
(415) 863-0600

Washington, D.C. Office
2200 Pennsylvania Avenue NW
4th Floor East
Washington, D.C. 20037
(202) 350-9992

New York Office
575 Madison Avenue
New York, NY 10022
(212) 315-2138

Los Angeles Office
1100 Glendon Avenue, 17th Floor
Los Angeles, CA 90024
(310) 689-7535

common sense®

www.commonsense.org

A. Maciel Printing