common sense®

2019 STATE OF EDTECH PRIVACY REPORT

Common Sense Privacy Program

Common Sense is the nation's leading nonprofit organization dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century.

common sense®

www.commonsense.org

Common Sense is grateful for the generous support and underwriting that funded this report from the Michael and Susan Dell Foundation, the Bill and Melinda Gates Foundation, and the Chan Zuckerberg Initative.

CREDITS

Authors: Girard Kelly
Jeff Graham
Jill Bronfman
Steve Garton

Suggested citation: Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). *2019 State of Edtech Privacy Report*. San Francisco, CA: Common Sense Media

This work is licensed under a Creative Commons Attribution 4.0 International Public License, excluding any copyrighted images contained within. All registered copyrights are the property of their respective owners. Cover image: © Getty Images.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The *2019 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 includes findings from evaluations of 150 privacy policies from the most popular edtech applications and services in 2019, as determined from interviews with various teachers, schools, and districts, as well as total App Store downloads during the past 12 months. The 2019 data is compared to our findings from 100 evaluations completed in 2018.

In addition, 2018 was a landmark year for privacy with a monumental shift in the focus and attention on the privacy practices of products used by consumers. Legislative initiatives such as the European-based General Data Protection Regulation (GDPR) and the corresponding California Consumer Privacy Act (CCPA) created a new narrative that highlighted the privacy shortcomings of big tech and social media companies, which led consumers to look more closely at the privacy practices of the products they use. These factors prompted vendors to update their policies at an unprecedented rate. Over half of the 100 most popular applications in 2018 had to be completely reevaluated due to these changes.

The good news is that the overall full evaluation median scores increased since 2018. There were also increases in the median scores for the privacy and security concerns of data collection, data sharing, data security, data rights, parental consent, and school purposes. In addition, there were increases in the median scores of privacy and security concerns that prohibit selling data, displaying advertisements, and tracking users. The following charts summarize our key findings:

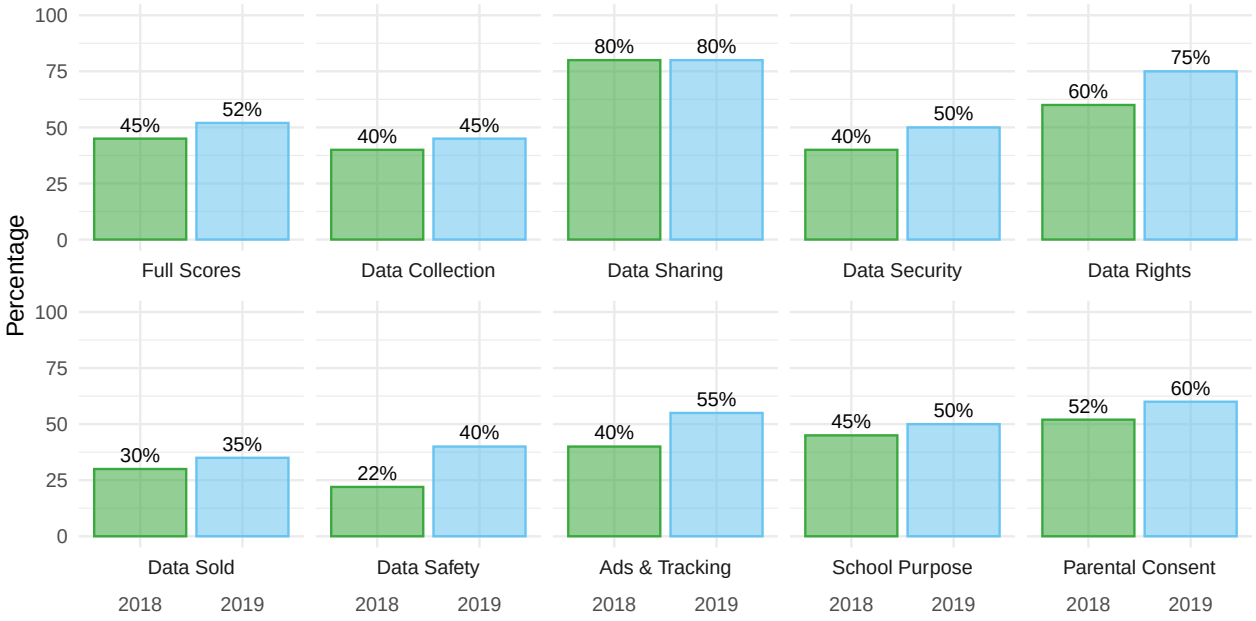


Figure 1: Key findings indicating median score changes from 2018 to 2019

While these increases in better practices are promising, there is still considerable work that needs to be done. There is a widespread lack of transparency and inconsistent and unclear practices for educational applications and other services targeted toward children and students. The majority of educational technology applications and services evaluated either do not adequately and clearly define safeguards taken to protect child or student information, or they lack a detailed privacy policy. While the number of products in our Use Responsibly Tier doubled from 10% to 20% since 2018 to meet our minimum safeguards, that still leaves 80% of applications and services not meeting this important threshold.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

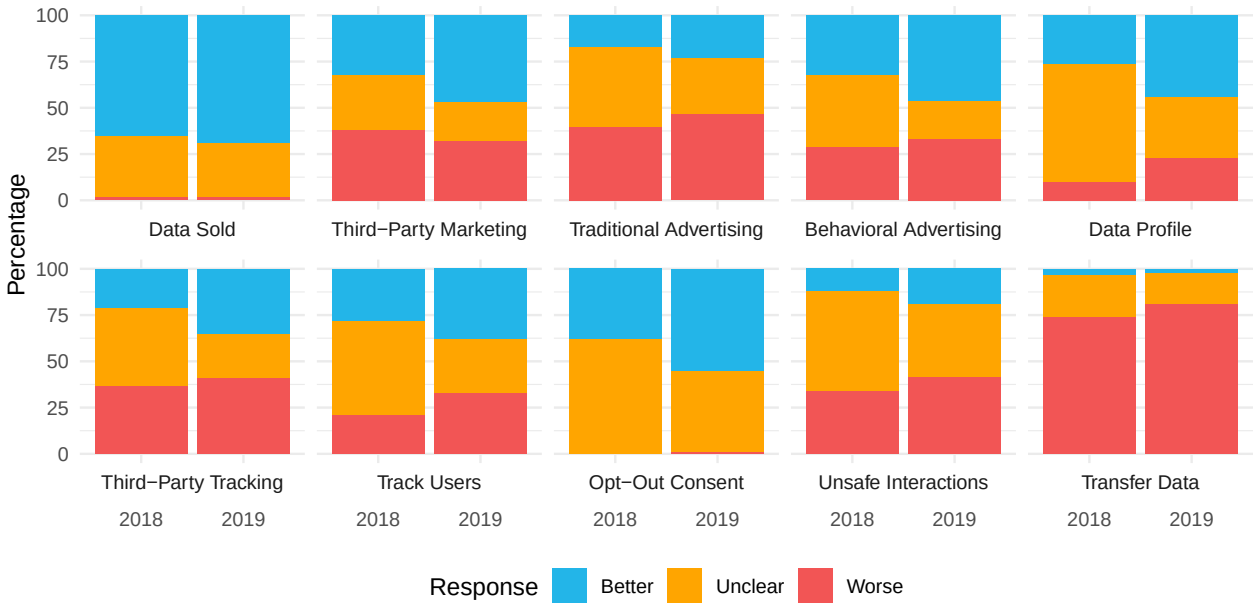


Figure 2: Key findings indicating changes in responses to tier-related questions from 2018 to 2019

The overall lack of transparency, which was pervasive across nearly all indicators we examined, is especially troubling. In our analysis, transparency is a reliable indicator of quality; applications and services that are more transparent also tend to engage in qualitatively better privacy and security practices. When these practices are not disclosed, there can be no standard of trust from 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 privacy landscape a particularly thorny one, marred by complex laws and statutes, technical issues and legacies, and keeping up with the changing needs of educators, students, and parents. Nevertheless, educational technology platforms serve an especially vulnerable population. Unfortunately, there is still far less attention paid to the privacy and security practices of technology platforms that affect tens of millions of children on a daily basis: educational software and other applications used in schools and by children outside the classroom. 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 updates and informs that critical conversation, and we intend to continue our research with annual updates and resources for the educational community on the state of edtech privacy.

INTRODUCTION

The Common Sense Privacy Program provides a framework to analyze and describe information in privacy policies so that 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. With the involvement of over 250 schools and districts, we are working in collaboration with third-party 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 our last *State of EdTech Report* was published in June 2018.[1] Since last year, we have spoken with numerous teachers, students, parents, developers, vendors, privacy advocates, and industry representatives about their perspectives on privacy.

The *2019 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 includes findings from evaluations of 150 privacy policies from the most popular edtech applications and services in 2019, as determined from interviews with various teachers, schools, and districts as well as total App Store downloads during the past 12 months. The 2019 data is compared to our findings from 100 evaluations completed in 2018. 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 for play and homework and by tens of millions of students in classrooms across the country. In order to effectively evaluate the policies of all these applications and services, a comprehensive assessment framework was developed based on existing international, U.S. federal, and U.S. state law, as well as privacy and security principles and industry best practices. This framework incorporates over 156 privacy- and security-related questions that are expected to be disclosed in policies for products used in an educational context. In addition, both qualitative and quantitative methods were developed, as described in our Methodology section, to determine both the particular issues vendors actually disclose in their policies and the meanings behind those disclosures.

Among the applications and services we evaluated for this report, some products did not have a privacy policy and/or terms of service available on their website at the time of our evaluation. In all cases where a mobile application was available, the products provided a link to the same privacy policy on their website from an app store. However, this report limits its analysis to only the policies of applications and services that were publicly available prior to use, as described in our Evaluation Process section of this report. As such, our analysis of applications that would fall under the "Not Recommended" tier are underrepresented in our analysis. Additionally our findings may not reflect all of the 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 add provisions as to how student information can be collected, used, and disclosed beyond the general provisions in the publicly available policies. In addition, many popular edtech applications or services that are not included in this report are available to the public without sufficient policies available. In many instances, popular edtech applications or services do not provide privacy policies prior to use, or provide broken links to missing policies, or do not contain policies at all. Since 2018 the Google Play and Apple App stores have started playing a leading role in improving the privacy practices of vendors by verifying that all applications in the "Kids Category" or "Designed for Families Program" must contain a link to a valid privacy policy and do not contain third-party targeted advertising, remarketing, and analytics.[2]

This report would not have been possible without support from the District Privacy Consortium, which includes over 250 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.[3] The findings in this report were prepared by the Privacy Program team members, including Girard Kelly, Jeff Graham, Jill Bronfman, and Steve Garton, who are leaders and experts in the fields of privacy and security with diverse backgrounds in entrepreneurship, computer science, ethics, law, academia, education, and public policy.

We believe that parents and schools can make better-informed decisions if provided with comprehensive and up-to-date information on the state of privacy for edtech applications and services. We believe that vendors and software developers can make better and safer products for chil-

1 Kelly, G., Graham, J., & Fitzgerald, B. *2018 State of Edtech Privacy Report*, Common Sense Privacy Evaluation Initiative. San Francisco, CA: Common Sense (2018), https://www.commonsense.org/education/articles/2018-state-of-edtech-privacy-report.

2 Sachdeva, K., *Building a safer Google Play for kids*, Android Developers Blog (May 29, 2019), https://android-developers.googleblog.com/2019/05/building-safer-google-play-for-kids.html; Apple, *Updates to the App Store Review Guidelines*, News and Updates (Jun. 3, 2019), https://developer.apple.com/news/?id=06032019j.

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

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

dren and students with this knowledge. 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 everyday and help support meaningful and positive changes in those practices. The following 2019 report illustrates our methodologies, results, categorical concerns, and key findings of privacy and security practices used by 150 popular edtech applications and services with comparisons to 100 evaluations completed in 2018.

Guidelines: A special note on how to use this report

- For **educators and district administrators**: The research summarized in this report started with the goal to address educators' needs and ends with this goal as well. We believe technology can augment existing educational practice for better learning outcomes. However, technology also poses some additional and unique challenges with maintaining a safe learning environment. You can use our report to make informed choices about the products you use in the classroom and pass on that information to students and families using apps at home.
- For **parents and guardians**: We encourage you to use the evaluations to choose more privacy-protective products for home use and to advocate for better products to be used in your children's classrooms. The results of this report may also inspire you to support legislation that protects child and student privacy at the local, state, and federal levels.
- For **policymakers and regulators**: This report is full of valuable data to support your legislative initiatives, regulatory rulemaking, and enforcement actions. The conclusions we have drawn in this report can reinforce your efforts to make the online marketplace safer for children and to support the educational mission of our schools.
- For **technologists and researchers**: When designing products used by children and students, this report will help guide your privacy-by-design decisions. Cost-effective and elegant design includes thinking about the needs of the user, and this report offers state-of-the-art privacy and security findings to meet those needs.
- For **privacy and security experts**: This report's analyses go beyond summarizing existing industry practices to forecasting industry trends and establishing best practices going forward. The statistics in this report can be used to support your work both to show the current level of disclosure and transparency and to imagine better solutions to the existing gaps in privacy and security communication between vendors and users.
- For **vendors and trade associations**: The overall findings in this report and our individual company privacy evaluations are both valuable tools to assess the industry on an ongoing basis. Further, we encourage vendors to view this data as a baseline and to increase the transparency and quality of privacy policies as part of your ongoing process of product improvement and to differentiate your privacy-forward applications and services from the industry at large.

Key Findings

Our overall findings in 2019 indicate a widespread lack of transparency and inconsistent privacy and security practices for products intended for children and students. However, since 2018, the state of edtech privacy has improved with the median overall privacy evaluation full scores increasing by approximately 15% to 52%. Higher scores are always better in our evaluation process, and this overall median full score is lower than expected, given these applications and services are intended for children and students. Our top key findings are illustrative of current privacy and security trends in the edtech industry that include several key areas of concern: Data Collection, Data Sharing, Data Security, Data Rights, Data Sold, Data Safety, Ads and Tracking, Parental Consent, and School Purpose.

The top 10 key findings are:

1

*The overall privacy evaluation **Full Scores** increased by 15%.*

An increase since 2018 in privacy evaluation median full scores generally indicates more transparent and qualitatively better practices disclosed in vendor's policies across a wide range of privacy, security, safety, and compliance concerns.

2

*The **Data Collection Scores** increased by 12%.*

An increase since 2018 in Data Collection median scores of applications and services indicates more transparent and qualitatively better practices related to protecting personal information.

3

*The **Data Sharing Scores** showed no change.*

No change since 2018 in Data Sharing median scores of applications and services indicates that companies did not update their policies in 2019 to disclose more transparent or qualitatively better practices related to protecting data from third parties.

4

*The **Data Security Scores** increased by 25%.*

An increase since 2018 in Data Security median scores of applications and services indicates more transparent and qualitatively better practices related to protecting against unauthorized access.

5

*The **Data Rights Scores** increased by 25%.*

An increase since 2018 in Data Rights median scores of applications and services indicates more transparent and qualitatively better practices related to controlling data use.

6

*The **Data Sold Scores** increased by 16%.*

An increase since 2018 in Data Sold median scores of applications and services indicates more transparent and qualitatively better practices related to preventing the sale of data.

7

*The **Data Safety Scores** increased by 45%.*

An increase since 2018 in Data Safety median scores of applications and services indicates more transparent and qualitatively better practices related to promoting responsible use.

8

*The **Ads and Tracking Scores** increased by 37%.*

An increase since 2018 in Ads and Tracking median scores of applications and services indicates more transparent and qualitatively better practices related to prohibiting the exploitation of users' decision-making process.

9

*The **Parental Consent Scores** increased by 15%.*

An increase since 2018 in Parental Consent median scores of applications and services indicates more transparent and qualitatively better practices related to protecting children's personal information.

10

*The **School Purpose Scores** increased by 11%.*

An increase since 2018 in School Purpose median scores of applications and services indicates more transparent and qualitatively better practices related to following student data privacy laws.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Tier Key Findings

Our evaluation tier-related findings indicate a widespread lack of transparency and worse privacy practices for products intended for children and students. However, since 2018, many of the criteria questions used in the Evaluation Tiers indicated an increase in transparency but disclosed both better and worse practices. Our top tier findings look at key evaluation tier criteria and related questions that include: Data Sold, Third-Party Marketing, Traditional Advertising, Behavioral Advertising, Data Profiles, Third-Party Tracking, Track Users, Opt-Out Consent, Unsafe Interactions, and the Transfer of Data.

The top 10 tier key findings are:

1

*The **Data Sold** question had better practices increase by 4%.*

Since 2018 we have seen an increase in the majority of applications and services that disclose they do not rent, lease, trade, or sell data, but many are still unclear.

2

*The **Third-Party Marketing** question had better practices increase by 15%.*

Since 2018 we have seen a significant increase in the majority of applications and services that disclose they do not allow third-party marketing, but many still disclose worse or unclear practices.

3

*The **Traditional Advertising** question had a 13% increase in transparency, but gains were roughly split disclosing both better and worse practices.*

Since 2018 we have seen a significant decrease in applications and services with unclear practices but also roughly equal increases in better and worse practices of traditional advertising.

4

*The **Behavioral Advertising** question had better practices increase by 14%.*

Since 2018 we have seen a significant decrease in applications and services with unclear practices and a significant increase in the majority of applications and services that disclose they do not allow behavioral advertising, but many still disclose worse or unclear practices.

5

*The **Data Profiles** question had a 31% increase in transparency with most of those gains (18%) disclosing better practices.*

Since 2018 we have seen a significant decrease in applications and services with unclear practices with most of the gains due to increases in better practices of creating advertising profiles, but many still disclose worse or unclear practices.

6

*The **Third-Party Tracking** question had better practices increase by 14%.*

Since 2018 we have seen a significant decrease in applications and services with unclear practices and a significant increase in applications and services that disclose they do not engage in third-party tracking, but many still disclose worse or unclear practices.

7

*The **Track Users** question had a 22% increase in transparency with most of those gains (12%) disclosing worse practices.*

Since 2018 we have seen a significant decrease in applications and services with unclear practices, with most of the gain in transparency being lost to increases in worse practices of tracking users across other websites.

8

*The **Opt-Out Consent** question had better practices increase by 17%.*

Since 2018 we have seen a significant decrease in applications and services with unclear practices and a significant increase in the number of applications and services that disclose that users can opt out from the disclosure or sale of their data to a third party.

9

*The **Unsafe Interactions** question had a 15% increase in transparency with roughly half of those gains (7%) disclosing better practices.*

Since 2018 we have seen a significant decrease in applications and services with unclear practices but also roughly equal increases in better and worse practices of unsafe interactions, but many still disclose unclear practices.

10

*The **Transfer Data** question had worse practices increase by 7%.*

Since 2018 we have seen a 6% decrease in applications and services with unclear practices but a 7% increase in the majority of applications and services that disclose they allow the onward transfer of data.

State of EdTech Trends

Our findings indicate that the state of edtech privacy has generally improved since 2018, with overall privacy evaluation scores increasing by approximately 15%. Our findings also indicate companies are slowly moving away from direct monetization and advertising using users' personal information, but they appear to be moving toward indirect advertising and monetization. This is a notable shift away from transparent practices of users viewing and clicking advertisements on the applications and services they use, to non-transparent practices of automatically collecting data from users and creating data profiles through third-party advertising tracking networks that display advertisements to users on other devices and applications and services across the internet.

This state-of-edtech trend is likely a compliance-motivated movement away from legally prohibited practices of selling personal information from children and students to third parties, or using their information to display behavioral advertising or for third-party marketing purposes. Also, this trend is likely influenced by the recent passage of numerous U.S. state student data privacy laws since 2018.[4] In addition, new consumer privacy laws were passed in 2018 and include Europe's General Data Protection Regulation (GDPR), which provides data rights and allows data subjects to withdraw consent or object to the sale of their personal information, and U.S state legislation such as the California Consumer Privacy Act (CCPA) provides consumers with the right to opt out of the sale of their personal information to third parties.[5] Accordingly, our results indicate a positive trend since 2018 in better disclosures in the following areas, addressed by our evaluation questions, allowing users to exercise their privacy rights: Access Data, Data Modification, User Deletion, User Export, and Opt-Out Consent.

Moreover, since 2018, more companies are disclosing that they engage in third-party tracking of users who use their products and that they allow third parties to use that information for their own purposes. This could be the result of the market for data tracking and analytics maturing and more options for companies looking to outsource this form of data monetization with more sophisticated offerings such as data profiling and long-game marketing. In addition, some vendors may be making this shift to a less transparent practice due to less regulation with respect to third-party data use and tracking as opposed to more regulated first-party data use and advertising. However, our findings also indicate a positive trend in many companies becoming more transparent in their policies to clarify their existing practices that disclose they do not engage in third-party tracking or profiling of their users.

[4] Future of Privacy Forum (FPF), *The Policymaker's Guide to Student Data Privacy* (Apr. 4, 2019), https://ferpasherpa.org/wp-content/uploads/2019/04/FPF-Policymakers-Guide-to-Student-Privacy-Final.pdf.

[5] *See* General Data Protection Regulation (GDPR), Regulation (EU) 2016/679; *See also* California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.198.

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 each 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 that same student's home address or other types of personal information. Therefore, our evaluation process pairs both a transparency evaluation with a qualitative evaluation, which provides the ability to track both which practices a policy discloses and the strengths and weaknesses of how a policy discloses that information in different contexts, as discussed further in the Privacy Concerns section. Lastly, our evaluation process includes reviewer-written summaries that highlight the implications of the application or service's privacy practices alongside the goals and contexts within which the service may be used. These summaries aid in the interpretation of our aggregate details as well as identify any shortcomings in our evaluation process relative to an individual product. More information about our privacy evaluations and summaries are available through the Common Sense Privacy Program website.[6]

Evaluation Process

The privacy evaluation process contains four steps:

1. **Overview**: Select a product and evaluate the details of the various policies of the application or service.
2. **Triage**: Answer brief observational questions not related to the policy text itself but rather relating to a superficial assessment of the vendor's privacy and security practices.
3. **Evaluation**: Answer questions about whether or not the text of the policies disclose particular issues. Questions are composed of the following details:
    a. **Transparency selection**: Do the policies address the issue(s) raised in the question?
    b. **Qualitative selection**: Do the policies indicate whether or not the vendor engages in the practice described?

[6] Common Sense Media, *Privacy Program*, https://privacy.commonsense.org/.

c. **Notes**: Is there anything noteworthy, exceptional, or egregious regarding the details of the question that should be noted?

d. **Policy references**: Can text within the policies be highlighted and associated with the particular question selected?

4. **Summary**: Create a general summary of the application or service and describe the relevant policy details.[7]

In addition to engaging in this evaluation process, our team also published a basic Information Security Primer.[8] While we do not run all these additional security-related tests as part of every evaluation, it's a useful resource, and we have used this primer to support multiple products addressing security issues.

Evaluation Framework

The privacy evaluation process includes questions organized into categories and sections derived from the Fair Information Practice Principles (FIPPs) that underlie international privacy laws and regulations.[9] In addition, the questions and the categories that organize them are all 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.[10] For example, the following evaluation question requires a reviewer to read the policies of the application or service and determine whether or not they disclose 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. 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 they engage in the particular practice described. A yes or no response that personally identifiable information is, or is not, collected will determine the final question points based on whether the practices described are considered qualitatively better or worse for the purposes of our evaluation process. Note that some questions do not have a qualitative component and are purely informational. This includes both questions where there is truly no qualitative value to a response and those questions where determining if a given response is qualitatively better or worse requires additional context outside the scope of the evaluation process. The Evaluation Scores section describes in more detail how responses to questions affect the overall roll-up score for an application or service.

Evaluation Details

Privacy evaluations are designed to categorize the complexity of a vendor's privacy policies into a simple and consistent framework that provides the right amount of detail and information about a product for every user and at the right decision point given their awareness and understanding of privacy. Our privacy evaluations aim to provide enough detail about a product based on a scale of a parent or educator's understanding of privacy to help them make a more informed decision and encourage all individuals to learn more about privacy and increase their awareness. The greater an individual's privacy awareness, the more detailed information displayed. The privacy evaluations categorize a parent or educator's privacy awareness into the following levels: no, low, medium, high, and compliance awareness.

No Awareness: These individuals have no awareness of privacy and do not consider privacy issues at all in their decision-making process.

Low Awareness: These individuals understand that privacy may be important but have minimal to no awareness of what privacy concerns or issues they should look for when deciding whether or not to use a product.

Medium Awareness: These individuals likely have never read a privacy policy but feel somewhat comfortable with their better-than-average understanding of a handful of important privacy risks and concerns that they always look for when evaluating whether or not to use a product.

High Awareness: These individuals are familiar with their most important privacy concerns about a product and are interested in reading detailed summary reports about a product to understand the risks. Also, these individuals are interested in learning more about complex privacy issues by reading our research reports.

Compliance Awareness: These individuals are considered "experts" by their peers and are comfortable reading privacy

7 Common Sense Media, *Evaluating Apps, Step By Step*, Privacy Program (2016), https://www.commonsense.org/education/privacy/blog/evaluating-apps-step-by-step; Common Sense Media, *Needles, Haystacks, and Policies*, Privacy Program (2017), https://www.commonsense.org/education/privacy/blog/needles-haystacks-policies.

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

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

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

policies and look for as much detail as possible about a product to meet their federal, state, or contractual procurement requirements.

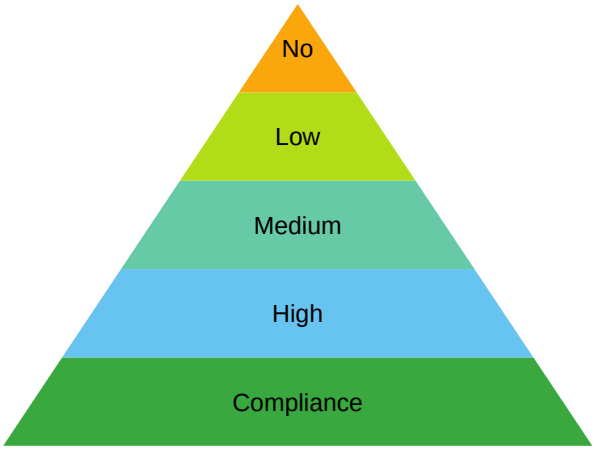


Figure 3: Hierarchical structure of user privacy awareness and privacy evaluation details

Table 1 describes how our privacy evaluations break down different levels of evaluation details based on an individual's privacy awareness:

Table 1: User awareness privacy evaluation details matrix

Awareness	Evaluation Details
No	Tier
Low	Basic Score, Tier Risk Flags
Medium	Product Summary, Product Concerns, Intended Users
High	Concern Score, Concern Statements, Standard Privacy Report
Compliance	Full Privacy Evaluation Reports, Full Privacy Evaluation Data Export

The Evaluation Tiers section describes how we categorize evaluations into three tiers based on meeting minimum privacy and security requirements, which parents and educators, with no privacy awareness, can use to make a more informed decision. Our Basic and Full Evaluations section describes the difference between basic and full evaluations, and our Basic Scores and Full Scores sections describe how a basic score relates to a full score to help parents and educators with low privacy awareness compare products and make an informed decision about a product's privacy practices alongside its evaluation tier. The Tier Risks section also describes how our tier criteria help parents and educators with low privacy awareness quickly understand why a product received its tier with some helpful information to learn more about the privacy risks and harms.

In addition, our evaluations provide a curated product summary, which parents and educators with medium privacy awareness can use to make a more informed decision with a little background and knowledge about how privacy and security work. Our product summaries generally describe the most important privacy-, security-, safety-, and compliance-related privacy issues about each product based on the concerns, as well as helpful links to the product's website, app store downloads, and privacy policy. Each evaluation also includes additional privacy and security concerns we have identified since 2018, as discussed in the Privacy Concerns section, which parents and educators with medium privacy awareness can use to learn more about a specific area of concern regarding a product. The Privacy Concerns section describes how parents and educators with medium privacy awareness can use different concerns—such as data collection, data security, data safety, or advertising—to make a more informed decision. Also, the Intended Users section describes what the policies specify are the intended users of an application or service, such as children, students, teens, parents, educators, or consumers.

For parents and educators with high privacy awareness, the Concern Scores section describes how each concern receives its own score based on how the company's policies answered the 10 questions in each concern. Similarly to tier risks, parents and educators can learn why each concern received the score it did with concern statements that automatically describe the practices of each question in a concern. The Standard Privacy Report section describes that for parents and educators with high privacy awareness, they can download a simple report that summarizes a product's policies in an easy-to-read bullet outline that describes the privacy statements of the product. Moreover, for parents, educators, and school or district administrators with compliance awareness of privacy, our full privacy evaluation reports and evaluation data export are available in a separate format for them to learn as much detail as possible about a product in order to meet their federal, state, or contractual procurement requirements. In addition, parents and educators with compliance awareness can navigate the privacy evaluation questions, which include additional background information and relevant citations to help them learn about better practices for each evaluation question.[11] Lastly, our policy annotator tool is available for parents, educators, and companies that would like to complete their own privacy evaluation and better understand the privacy practices of products they use everyday.[12]

[11] Common Sense Media, *Full Privacy Evaluation Questions*, Privacy Program, https://privacy.commonsense.org/resource/full-evaluation-questions.

[12] Common Sense Media, *Policy Annotator*, Privacy Program, https://policy-annotator.commonsense.org.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Procedural Changes

The largest difference between our 2018 and 2019 analyses is our shift from analyzing only transparency and nontransparency to indicating yes or no responses in 2019 data. Unfortunately, our evaluation-data snapshot from 2018 does not include this additional nuance, so some question analysis will indicate "transparent" for 2018 data only. This set of "transparent" responses is comparable to both the yes responses and the no responses from 2019. While this comparison is awkward for this second-year analysis, we feel this provides a more complete understanding of industry practices and will enable better analysis of trends in future years.

Beyond that change, we have made several other adjustments to the analysis process since 2018 that warrant a brief mention here:

1. Statutory analysis now includes additional analysis beyond just a brief mention of COPPA and our evaluation process' capabilities for more narrowly focused analysis. Please review the Statute Scores section for additional details and deeper analysis of industry shifts from 2018 to 2019.
2. Inclusion of both a basic score and a full score. In 2018 we launched our basic evaluations, composed of a carefully selected set of 34 questions intended to provide greater coverage of products. In several areas we provide a breakdown between a full score and a basic score. It should be understood that a full score always includes responses to the full 156-question set whereas a basic score only uses the 34 questions included in our basic evaluation process. When comparing a basic score to a full score, the intent is to provide insight into where a basic score can provide accurate prediction into what a product's full score for a particular overall, concern, or statutory score might be. Please refer to the Privacy Concerns, Statute Score, or Regression Analysis sections of basic-to-full concern score comparisons for further details concerning which basic concern scores are reliable predictors of full concern scores.
3. Most analyses use bar charts for comparing 2018 and 2019 individual question responses. In order to provide better insight in comparing 2018 and 2019 question response trends, we have switched to using bar graphs with series trend data to better indicate trends and shifts over time in question response data.
4. Additionally, we have moved to using box plots for comparing 2018 and 2019 data, as they provide a data-rich visualization for understanding how the industry responses are distributed. As a brief refresher, box plots partition a population into groups of 25% (or quartiles).
    a. The lower or first quartile is represented by the portion of the graph between the lower whisker and the lower boundary (Q1) of the shaded area.
    b. The second quartile is represented by the lower portion of the shaded area from the lower boundary (Q1) on the lower side and the upper boundary (Q2) or the median.
    c. The third quartile is represented by the upper portion of the shaded area from the lower boundary (Q2), or the median, on the lower side and the upper boundary (Q3).
    d. The fourth quartile is represented by the upper portion of the graph between the upper whisker and the upper bound (Q3) of the shaded area.
    e. Outliers are denoted as single points outside the whiskers. These are scores that are either considerably above industry norms if above the fourth quartile or considerably below industry norms if below the first quartile.

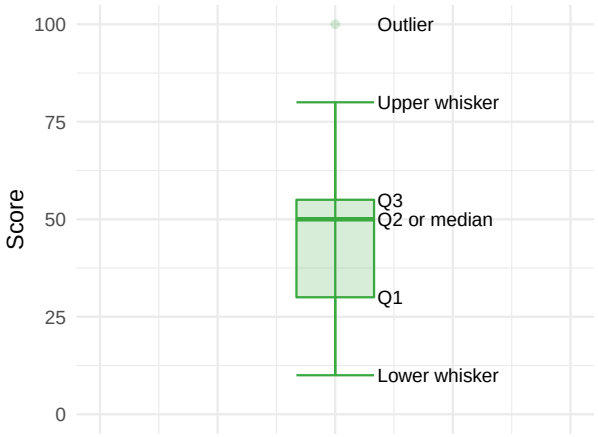


Figure 4: Example box plot

Basic and Full Evaluations

Basic evaluations and full evaluations both have the same tier names and use the same tier questions but designate whether the evaluation is a basic or full evaluation below the tier name and icon. Basic evaluations are a 34-point inspection of the most important privacy and security questions about a product.[13] Full evaluations are a 156-point inspection of the comprehensive privacy and security questions about a product.[14] Basic evaluations answer the most critical

[13] Common Sense Media, *Basic Evaluation Questions*, Privacy Program, https://privacy.commonsense.org/resource/basic-evaluation-questions.

[14] Common Sense Media, *Full Evaluation Questions*, Privacy Program, https://privacy.commonsense.org/resource/full-evaluation-questions.

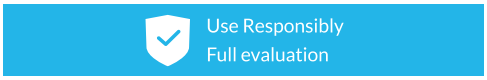
privacy and security questions about a product to determine a basic score, concern scores, and which evaluation tier they belong to in order to allow parents, teachers, schools, and districts to make an informed decision about whether to use the product. Basic evaluations do not answer all the questions of a full 156-point inspection evaluation of a product and therefore do not display a full evaluation score or full concern scores. However, basic evaluations can still be compared to full evaluations because they share Basic Scores, basic Concern Scores, Evaluation Tiers, and a subset of the Standard Privacy Report.

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 the specific needs and the decision-making process of schools and districts into the following three tiers[15]:

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 or guarantee 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.

Use Responsibly



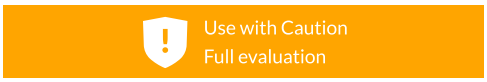
Meets our minimum requirements for privacy safeguards, but more research should be completed prior to use.

Applications and services in the Use Responsibly tier have met a minimum criteria for transparency and qualitatively better practices 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 application or service. In addition, a more detailed review should happen before any child or student data is shared with a service.

In 2019, approximately 20% of applications and services are designated Use Responsibly, which is a 10% increase in the percentage of products with overall better tier question practices since 2018. Responses to the questions listed below are displayed to provide more detail about a product in the Use Responsibly tier:

1. Do the policies clearly indicate whether or not the product is intended to be used by children under the age of 13?
2. Do the policies clearly indicate whether or not the vendor limits the collection or use of information to only data that is specifically required for the product?
3. Do the policies clearly indicate whether or not a user can interact with trusted users?
4. Do the policies clearly indicate whether or not a user's personal information can be displayed publicly in any way?
5. Do the policies clearly indicate whether or not the vendor provides notice in the event of a data breach to affected individuals?
6. Do the policies clearly indicate whether or not the vendor or third party obtains verifiable parental consent before they collect or disclose personal information?

Use with Caution



Does not meet our minimum requirements for privacy safeguards, and more research should be completed prior to use.

Applications and services in the Use with Caution tier have issues narrowly focused around data use 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 for advertising purposes can potentially violate multiple state laws and in some cases federal law. An application or service can be designated Use with Caution for either 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. Unclear or qualitatively worse responses to the questions listed below trigger inclusion in the Use with Caution tier:

1. Do the policies clearly indicate the version or effective date of the policies?

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

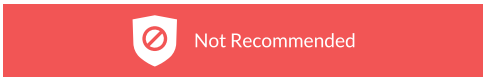
CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

2. Do the policies clearly indicate whether or not a user's personal information is sold or rented to third parties?
3. Do the policies clearly indicate whether or not a user's personal information is shared with third parties for advertising or marketing purposes?
4. Do the policies clearly indicate whether or not behavioral or contextual advertising based on a user's personal information is displayed?
5. 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. 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. Do the policies clearly indicate whether or not the vendor allows third parties to use a user's data to create a profile, engage in data enhancement or social advertising, or target advertising?

An evaluation designation of Use with Caution is not necessarily a sign that a vendor is doing anything illegal or unethical, but it could mean, based on how the application or service is used, that it may be violating either federal or state law. 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 users with ads based on the users' activities and behavior ("behavioral ads").

In 2019, approximately 60% of applications and services are designated Use with Caution, which is a 20% decrease from 2018 in the percentage of products designated User with Caution. However, this decrease was due to a respective 10% increase in the number of applications and services designated Use Responsibly and Not Recommended. On the bright side, a majority of applications and services (68%) disclosed that they do not rent, lease, trade, or sell data. However, a majority of applications and services are unclear or explicitly allow Third-Party Marketing, Behavioral Advertising, and Third-Party Tracking, Track Users across other websites, or allow the creation of Data Profiles. This use of educational data for noneducational purposes, even if legal, is contrary to user expectations about edtech.

Not Recommended



Fails to meet our fundamental requirements for privacy safeguards, which include encryption and a detailed privacy policy.

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. Unclear or qualitatively worse responses to 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?
4. Does the product use trackers on its homepage, on its registration page, or while a user is logged in?

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 four 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. In 2019, approximately 20% are designated Not Recommended, which is a negative trend since 2018 and a 10% increase in the percentage of products with overall worse tier question practices since 2018. This increase is likely the result of a more representative selection of applications and services evaluated in 2019. Among the applications or services we evaluated, only a small number did not have a privacy policy and/or terms of service available on their website at the time of our evaluation. Nonetheless, as with the Use with Caution criteria described above, a Not Recommended designation is not a sign that a vendor is necessarily doing anything illegal or unethical, but it could mean, based on how the application or service is used, that it could be violating either federal or state laws. It is a sign that, based on publicly available policies and observed security practices, their services do not provide adequate guarantees that information stored in their information systems will be protected.

Tier Risks

As described above, the Common Sense Privacy Program helps parents, teachers, schools, and districts make sense of the privacy risks they may face with our Evaluation Tiers that flag areas of concern. A comprehensive privacy risk assessment can identify these risks and determine which personal information companies are collecting, sharing, and using to minimize potential harm to children and students. Children require specific protection of their personal information, be-

cause they may be less aware of the risks, consequences, safeguards, and concerns and their rights in the processing of their personal information. These protections should apply to the use of personal information of children for the purposes of marketing or creating personality or user profiles and the collection of personal data from children when using services offered directly to a child.[16]

The Privacy Program provides an evaluation process that assesses what companies' policies say about their privacy and security practices. Our evaluation results, including the easy-to-understand tier icons described above, indicate which companies are transparent about what they do and don't do but also indicate whether a company's privacy practices and protections meet industry best practices.

Beyond the overall tier icons, Common Sense privacy evaluations display evaluation tier criteria for each product and indicate when a criteria is found to be a worse or unclear practice with a yellow alert icon. These yellow alert icons, illustrated below, give a clear indicator of which factors deserve more scrutiny. Looking at this list, the potential user can see which of the vendor's practices caused us some concern. We realize that educators' time is short and we strive to communicate the results of our privacy evaluations in a scalable way. This level of information is more detailed than the tier ratings and allows those who are curious about why we gave a product a particular tier rating to see which factors deserved special notice and are therefore marked with a yellow alert icon.

- Privacy policies do indicate a version or effective date.
- Data are not sold or rented to third parties.
- Data are not shared for advertising or marketing.
- Behavioral or contextual advertising is not displayed.
- ⚠ Data are collected by third-party advertising or tracking services.
- ⚠ Unclear whether this product uses data to track and target advertisements on other third-party websites or services.
- ⚠ Unclear whether this product allows third parties to use data to create ad profiles, data enhancement, and/or targeted advertisements.

Figure 5: Example of tier risks shown on a privacy evaluation.

The following evaluation tier criteria describe some of the most important privacy risks and resulting harms that can occur with technology products intended to be used by children and students. These risks also affect their parents and educators, both directly as users themselves and indirectly in that their children and students are harmed by privacy risks.

Not Recommended Criteria

The following criteria are used in the determination of whether or not a product receives a Not Recommended tier designation for lack of a privacy policy or encryption to protect children's and students' personal information.

Privacy Policy: The privacy policy for the specific product (vs. a privacy policy that just covers the company website) must be made publicly available. Without transparency into the privacy practices of a product, there are no expectations on the part of the child, student, parent, or teacher of how that company will collect, use, or disclose collected personal information, which could cause unintended harm.[17]

Supporting Encryption: A product is required to use and/or redirect all pages to encryption with HTTPS. Without basic security protections, such as encryption of personal information while in transit, there is an increased risk of potential interception and misuse of personal information (by unauthorized third parties) that may include a child or student's login credentials, which could cause unintended harm. Unencrypted product pages can be tampered with to look official and appear to be coming from an official source, which could enable phishing attacks or leaking of sensitive information.

Use with Caution Criteria

The following criteria are used to determine whether a product receives a Use with Caution tier designation for unclear or worse practices.

Data Sold: A child or student's personal information should not be sold or rented to third parties. If a child or student's personal information is sold to third parties, then there is an increased risk that the child or student's personal information could be used in ways that were not intended at the time at which that child or student provided their personal information to the company, resulting in unintended harm.

Third-Party Marketing: A child or student's personal information should not be shared with third parties for advertising or marketing purposes. An application or service that requires a child or student to be contacted by third-party companies for their own advertising or marketing purposes increases the risk of exposure to inappropriate advertising and influences that exploit children's vulnerability. Third parties who try to influence a child's or student's purchasing behavior for other goods and services may cause unintended harm.

Behavioral Advertising: Behavioral or contextual advertising based on a child or student's personal information should not be displayed in the product or elsewhere on the internet. A

16 *See* General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

17 Kelly, G., Graham, J., Bronfman, J., & Garton, S. *Privacy risks and harms*, San Francisco, CA: Common Sense Media (2019).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

child or student's personal information provided to an application or service should not be used to exploit that child or student's specific knowledge, traits, and learned behaviors to influence their desire to purchase goods and services.

Third-Party Tracking: The vendor should not permit third-party advertising services or tracking technologies to collect any information from a user of the application or service. A child or student's personal and usage information provided to an application or service should not be used by a third party to persistently track that child or student's actions on the application or service to influence what content they see in the product and elsewhere online. Third-party tracking can influence a child or student's decision-making processes, which may cause unintended harm.

Tracking Users: A child or student's personal information should not be tracked and used to target them with advertisements on other third-party websites or services. A child or student's personal information provided to an application or service should not be used by a third party to persistently track that child or student's actions over time and across the internet on other devices and services.

Data Profile: A company should not allow third parties to use a child or student's data to create a profile, engage in data enhancement or social advertising, or target advertising. Automated decision-making, including the creation of data profiles for tracking or advertising purposes, can lead to an increased risk of harmful outcomes that may disproportionately and significantly affect children or students.

Use Responsibly Details

If a product does not activate any of our criteria for the Not Recommended or Use with Caution tiers, it has met our **minimum** safeguards and is designated Use Responsibly. Since the Use Responsibly tier does not have explicit criteria of its own, we highlight the following practices: limiting the collection of personal information, making information publicly visible, safe interactions, data breach notification, and parental consent.

Children Intended: A vendor should disclose whether children are intended to use the application or service. If policies are not clear about who the intended users of a product are, then there is an increased risk that a child's personal information may be used in ways that were not intended at the time at which that child provided their personal information, resulting in unintended harm.

Collection Limitation: A company should limit its collection of personal information from children and students to only what is necessary in relation to the purposes of providing the application or service. If a company does not limit its collection of personal information, then there is an increased risk that the child or student's personal information could be used in ways that were not intended, resulting in unintended harm.

Visible Data: A company should not enable a child to make personal information publicly available. If a company does not limit children from making their personal information publicly available, there is an increased risk that the child or student's personal information could be used by bad actors, resulting in social, emotional, or physical harm.

Safe Interactions: If a company provides social interaction features, those interactions should be limited to trusted friends, classmates, peer groups, or parents and educators. If a company does not limit children's interactions with unknown individuals, there is an increased risk that the child or student's personal information could be used by bad actors, resulting in social, emotional, or physical harm.

Data Breach: In the event of a data breach, a company should provide notice to users that their unencrypted personal information could have been accessed by unauthorized individuals. If notice is not provided, then there is an increased risk of harm due to the likelihood of personal information that was breached being used for successful targeted or phishing attempts to steal additional account credentials and information, resulting in potential social, emotional, or physical harm.

Parental Consent: A company should obtain verifiable parental consent before the collection, use, or disclosure of personal information from children under 13 years of age. If parental consent is not obtained, then there is an increased risk that the child or student's personal information could be inadvertently used for prohibited practices, resulting in unintended harm.

Intended Users

An application or service can have many intended users or just one type of specific intended user. For example, some products are designed for a general audience that does not include kids, but other products are designed to be used exclusively by children or students. In addition, some products are designed for a mixed audience and are intended to be used by anyone including children, teens, students, parents, educators, and consumers.

General Audience Product

A general audience product is a product intended for adults where the company 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 prior to the collection or use of information.[18] For example,

[18] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

a product that is not intended for children and would not likely appeal to children under 13, such as a tax preparation service, would be a general audience product.

However, a general audience product may be considered directed to children if the product would appeal to children under 13 years of age, which takes several factors into consideration such as: the subject matter, visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, the age of models, the presence of child celebrities or celebrities who appeal to children, language or other characteristics of the product, or whether advertising promoting or appearing on the product is directed at children.[19] Therefore, a general audience application or service that collects personal information from users to teach them ABCs or basic numbers with animated cartoon characters would likely be a child-directed product.

Mixed-Audience Product

A mixed-audience product is directed to children but does not target children as its "primary audience" but rather targets teens 13 to 18 years of age or adults. A mixed-audience product is required to obtain age information from any user before collecting any personal information. In addition, if a user identifies themselves as a child under the age of 13, the company must obtain parental consent before any information is collected or used. For example, an education or consumer product that allows parents or teachers to log in through a separate account to use the product themselves, or to monitor or manage their children or student's accounts, would be a mixed-audience product.

Child-Directed Product

A product directed at children is a product where the company has actual knowledge it is collecting information from children under the age of 13 because children are targeted as the primary audience, and, as a result, parental consent is required before the collection or use of any information. For example, an application or service that teaches ABCs or basic numbers with animated cartoon characters would be a child-directed product.

Differential Privacy

The Privacy Program only evaluates products that are for a mixed audience that includes kids, or products directed at children and students. A child-directed product typically has a unique privacy policy and website, and the application or service has the same privacy protections for both children and students. However, mixed-audience products with various users often have different privacy practices and protections based on the category of user. This type of differential privacy allows the company to establish privacy protections that apply only to a specific subset of users. Companies' goal is to limit the privacy protections to as few individuals as possible. For example, some products may sell user data and display behavioral advertising to parents, teachers, and consumers but not do so for children or students.

The Privacy Program evaluates products based on multiple dimensions that include an overall score, evaluation tiers, and evaluation concerns, as described in our Evaluation Details section. A product's overall score can be used by all intended users of a product to better understand its privacy protections and to more easily compare products based on how well they protect the privacy of all users. In addition, a product's tier can be used by all intended users of a product to understand potential issues with a product's privacy practices. This is an important feature of our privacy evaluations because if a mixed-audience product is intended for both children and adults but has different privacy practices for adults than kids, our evaluation tier reflects any "worse" practices—for the purposes of our evaluation process—because it applies to any intended user of the product. Additionally users may automatically change class as they use a product and lose protections that were formerly in place. For example, if a product has greater protections for kids under 13, when a kid turns 14 they may no longer benefit from the additional protections afforded to users under the age of 13. As a result our evaluations focus on the details that apply generally or apply to all users, as a user may not have control over the conditions that determine which protections they and their data are afforded.

Protecting Users

Our evaluation tiers are designed to protect all users and flag a privacy risk if it applies to any intended user of the product. The following three examples illustrate the different evaluation tiers a mixed-audience product could receive:

1). **No tier flags.** If none of the Use with Caution tier criteria has been flagged with an alert icon, that means the answers to all the tier questions have been disclosed in a product's policy with "better" responses for the purposes of our evaluation. This product would receive a Use Responsibly tier icon.

2). **Tier flags apply to all users.** If one or more of the Use with Caution tier criteria has been flagged a privacy risk, that product would be designated Use with Caution—for example, if a product's terms state that personal information from any user may be sold to third parties or used to display behavioral advertisements or tracking purposes.

[19] FTC, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

3). **Tier flags apply to only a specific type of user.** If one or more of the Use with Caution tier criteria has been flagged a privacy risk, that product would be designated Use with Caution. However, if the privacy risks only apply to a specific type of intended user such as a parent or educator but do not apply to children and students, the product would still be designated Use with Caution. This approach alerts all intended users of the potential privacy risks but also indicates in the product's overall summary any additional protections provided for other intended users—for example, if a product's terms state that no personal information collected from children or students using the product may be sold to third parties or used to display behavioral advertisements, but other intended users such as parents or educators do not have similar protections.

We believe this approach better protects children and students when using products with different privacy practices based on the type of user, because rather than provide a false impression of safety for all users when only one group of intended users is afforded protections, we display the potential issues if any intended users are at risk. This allows parents and educators to be better informed about a product's overall privacy risks up front and provide them the opportunity to learn more about how a product's privacy risks may affect their own decision to use a product based on their unique concerns. Moreover, this approach also allows parents and educators to make an informed decision with all the available information on whether a product may still be appropriate to use in their context because it protects the personal information of children and students differently.

Standard Privacy Report (SPR)

The standard privacy report (SPR) displays the most important privacy practices from a product's policies in a consistent easy-to-read outline. The SPR indicates whether or not a product's policies disclose that they engage in each particular privacy practice and displays an alert when users should further investigate particular details prior to use. This alert indicates that the particular practice is risky, unclear, or has not been evaluated. The SPR shows 80 of the most significant findings from our full 156-question evaluation framework. The SPR also includes all the basic evaluation questions and is available for both a basic and full evaluation of a product. The SPR does not summarize a full evaluation but rather provides a representative sample of the full evaluation findings as well as all of the basic evaluation findings for easier comparison among products. A sample SPR is provided below:

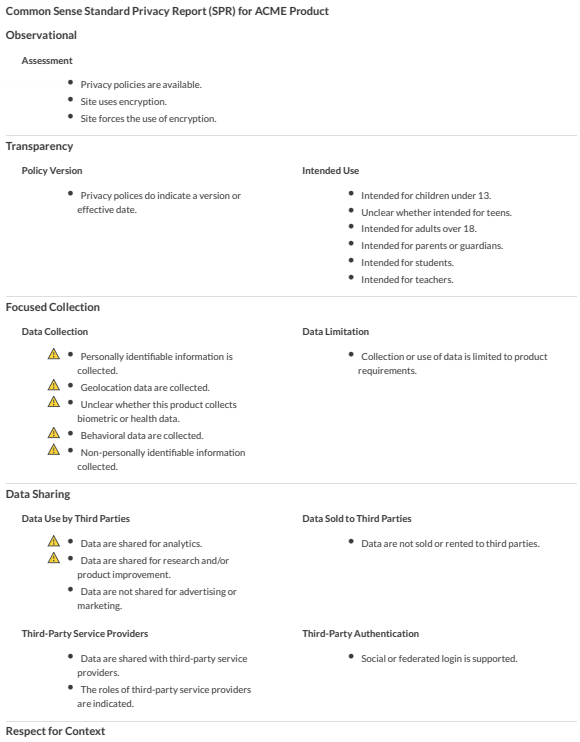


Figure 6: Example of a Standard Privacy Report (SPR) for a privacy evaluation.

There are several options for navigating the questions and learning more about data privacy. You can view all the SPR core questions with each of their possible answers for yes, no, unclear, and not evaluated.[20] In addition, you can navigate the privacy evaluation questions, which include additional background information and relevant citations to help understand each possible answer in the SPR to learn about better practices for each evaluation question. [21]

Evaluation Updates

The Privacy Program monitors thousands of companies' privacy policies in order to detect any change or update in the language of the policy. This process allows us to check whether any additions or deletions to a policy are trivial or substantive in nature and to update that company's privacy evaluation to reflect any changes in that product's privacy practices. Typically a company will update their privacy policy once a year, or once every two years, with a minor change to their contact information, new hyperlinks, or clarification of headings and section numbers. When substantive changes

[20] Common Sense Media, *Standard Privacy Report Questions*, Privacy Program, https://privacy.commonsense.org/resource/standard-privacy-report-questions.

[21] Common Sense Media, *Full Privacy Evaluation Questions*, Privacy Program, https://privacy.commonsense.org/resource/full-evaluation-questions.

are made, typically the changes are additions to the policy text that improve transparency around privacy practices the company may already engage in. From our informal observation of changes to privacy policies, substantive changes to a policy typically result in 20% to 30% of the policy text changing compared to the previous version. Companies choose to make substantive changes to their privacy policies based on many factors, but typically we see changes made in response to customer questions about that company's specific practices, or the addition of new features or products that change how the company collects or uses personal information, or for compliance purposes with changes in the law.

In the summer of 2018, companies made substantive changes to their privacy policies at a rate higher than seen in previous years. For example, the Privacy Program found that 56% of the 150 most popular edtech applications and services made substantive changes to their policies in 2018 with many policies changing more than 60%, including both additions and deletions. In some cases, companies updated their policies several times in 2018. Users may have received email notifications that the company's policies had changed, seen app notifications that required them to consent to new policies, or noticed changes to the effective date, versions, and hyperlinks of the policies. The reason why such a high percentage of companies updated their policies in 2018 was several important privacy developments that occurred during 2018.

Many companies updated their policies for compliance purposes to incorporate new privacy rights granted by changing U.S. state or international laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018 and provided many new privacy rights for companies subject to the GDPR's requirements.[22] In addition, California passed the California Consumer Privacy Act (CCPA), which provided many of the same privacy rights as the GDPR for California citizens, as well as the right for consumers to provide opt-out consent from a company selling their personal information.[23] At least eight other U.S. states also passed privacy laws in 2018 including: Hawaii, Maryland, Massachusetts, Mississippi, New Mexico, New York, North Dakota, and Rhode Island. As a result, many privacy policies included additional language to be more transparent and disclose better practices in 2018. Accordingly, our 2019 results indicate a positive trend since 2018 in better disclosures for the following evaluation questions related to new legislative requirements that allow users to exercise their privacy rights: Access Data, Data Modification, User Deletion, User Export, and Opt-Out Consent. In addition, many companies updated their policies around third-party practices of Data Shared, Sharing Purpose, and Reasonable Security in response to consumer awareness and complaints. Throughout 2018, there was national media attention focused on numerous data breaches affecting hundreds of millions of consumers and on privacy scandals involving data misuse, such as Facebook and Cambridge Analytica.[24]

Evaluation Scores

After numerous conversations over the past year explaining our work to vendors, district technology coordinators, parents, and teachers, it became clear we needed a more transparent and simpler method to explain our process for calculating basic and full scores.

Prior to 2019 we used a complex score-calculation process that included:

1. A hierarchical relationship of questions to influence whether or not other additional questions were expected to be answered;
2. Five weight categories to indicate which questions were more or less important; and
3. A separation of transparency and quality scores

While our current process for interpreting our evaluation scores is not as nuanced as our previous process, we found that in general the variation between our previous and current methodology provided very little, or only a negligible, difference in the resulting score. Where larger differences in scores were found, the difference was typically in a direction that reflected what the data was informing rather than skewed based on incentivized responses for a narrow set of questions. Either method of calculating aggregate scores results in the same interpretation; higher scores indicate products that are attempting to be transparent in all contexts and are typically disclosing qualitatively better practices, whereas lower scores indicate products that are not transparent or require more work from a prospective user to determine the privacy practices of the given product.[25] Our new scoring methodology still provides an incentive for companies to be more transparent about their practices. We feel that making informed decisions, regardless of the ultimate practices of a product, is critical for effective privacy and for user agency. As such, our new scoring method now expects all questions to be answered. For each question, the scoring is as follows:

22 *See* General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

23 California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.198.

24 Rosenberg, M., Confessore, N., and Cadwalladr, C. *How Trump Consultants Exploited the Facebook Data of Millions* (Mar. 15, 2017), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

25 Common Sense Media, *Evaluation Scores*, Privacy Program (2018), https://privacy.commonsense.org/resource/evaluation-scores.

Table 2: Question scoring matrix

Score	Question Response
0.0	Not transparent or unclear
0.5	Transparent, but response is qualitatively worse
1.0	Transparent, and if question has a qualitative component, the response is qualitatively better

This improved scoring methodology dramatically simplifies our scoring process such that each question contributes one point to the overall possible score and a score is calculated by totaling the points earned for a given set of questions relative to the number of questions in consideration. This allows us to take any subset of questions and generate a score. As described above, a score is calculated by taking the total number of points earned and dividing by the number of questions in consideration. This provides a percentage that allows for easier interpretation across different facets of an evaluation. For instance, our basic evaluation score is composed of 34 questions, whereas our full evaluation score is calculated against 156 questions. Similarly, our concern scores utilize 10 questions and statute scores are calculated against the respective number of questions in each breakdown.

Statute Scores

Each statute or regulation is associated with one or more evaluation questions. As such, we can calculate scores for each statute or regulation using only those questions associated with the statute or regulation. Each specific statute or regulation's score serves as an indirect proxy indicating the likelihood of the application or service satisfying all of its compliance obligations.

Table 3: 2019 statute score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
COPPA	8	46	55	53	63	83
FERPA	6	39	50	49	60	81
SOPIPA	9	46	57	56	69	86
GDPR	18	52	59	60	71	86
Data breach	0	25	50	60	100	100
AB 1584	0	40	60	58	79	100
CalOPPA	31	62	71	68	77	85

However, this statute or regulation score only provides an indication of how much additional work may be required to determine whether an application or service is actually in compliance with applicable federal or state law in a specific context. A score of less than 100 indicates that additional information is likely required to determine whether an application or service is compliant in all contexts. A lower overall statute 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. In general, lower scores indicate more work would be necessary to ensure the appropriateness of the application or service in each particular context. On the other hand, a higher score indicates that various contexts are more likely to include the necessary information to determine whether compliance is satisfied for that particular use. Each application or service's legal obligations should only be understood in the context in which it is used.

The following statute score analysis illustrates some of the most important privacy laws affecting children, students, parents, and teachers. Each comparison chart below is a box plot and described further in the Procedural Changes section.

Children's Online Privacy Protection Act (COPPA)

Figure 7 illustrates the statute scores for COPPA, which is a federal law with many requirements that includes that the application or service must obtain parental consent before the collection or disclosure of personal information from children under 13 years of age.[26] Table 4 compares and summarizes the COPPA statute score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 4: 2018 vs. 2019 COPPA score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	7	35	47	45	55	82
2019	8	46	55	53	63	83

From the analysis of COPPA-related questions, which represent approximately 50% of all our questions, we determined a median in 2019 of approximately 55%. This median is lower than expected, given that these applications and services are intended for children and students and that a majority of companies disclose qualitatively better practices and limit the collection of personal information and obtain parental consent before the collection or disclosure of personal information from children under 13 years of age. However, this lower COPPA statute score may be attributable to applications and services that disclose they are not intended for children under 13 years of age but still target or appeal to children under 13 years of age. Comparatively, the COPPA minimum, median, mean, and maximum are similar to the other

[26] *See* Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501-6508.

statute scores analyzed for this report, which may indicate that the majority of applications and services are only focusing on disclosing minimum compliance requirements.

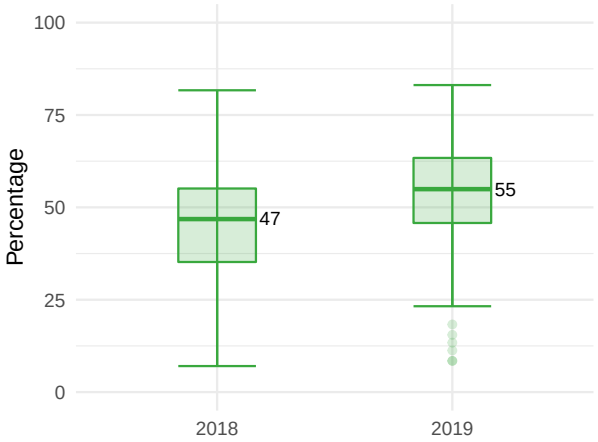


Figure 7: Comparison of Children's Online Privacy Protection Act (COPPA) scores year over year

Compared to 2018, applications and services evaluated in 2019 indicate a 17% increase in median COPPA scores that indicate more transparent and qualitatively better practices regarding the collection and disclosure of personal information from children under 13 years of age. In addition, since 2018 the industry has improved its practices regarding COPPA compliance, as seen by the 2019 median of approximately 55% moving beyond the third quartile of the 2018 range of scores. Lastly, because the industry has improved its COPPA compliance-related practices since 2018, there are now several outliers that are denoted with circles in 2019. These applications or services are now considered below the range of industry best practices and should update their terms accordingly.

Family Educational Rights and Privacy Act (FERPA)

Figure 8 illustrates the statute scores for FERPA, which is a federal law with many requirements that protects the privacy of student education records.[27] Table 5 compares and summarizes the FERPA statute score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

[27] *See* Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, 34 CFR Part 99.

Table 5: 2018 vs. 2019 FERPA score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	6	29	42	40	51	79
2019	6	39	50	49	60	81

From the analysis of FERPA-related questions, we determined a median in 2019 of approximately 50%. This median is lower than expected and lower than the median COPPA statute score, given that these applications and services are intended for students and that a majority of companies disclose the qualitatively better practice that a parent or guardian can request the educational agency to access, modify, or delete their student's education records. However, this low median statute score may be the result of companies that enter into contracts or student data privacy agreements with schools and districts and require the school or district to control the collection of personal information, parental consent, and subsequent requests to access and review that data from eligible students, teachers, and parents. These companies may assume that because the contract discloses that the school, district, or faculty controls the deployment of the application or service and administration of student accounts that they do not also need to disclose those practices in their policies.

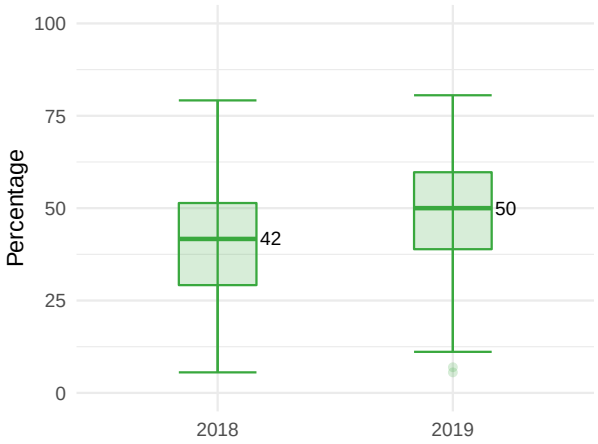


Figure 8: Comparison of Family Educational Rights and Privacy Act (FERPA) scores year over year

Compared to 2018, applications and services evaluated in 2019 indicate a 21% increase in FERPA median scores that indicate more transparent and qualitatively better practices regarding parents and eligible students' rights to access, modify, or delete the student's education records. In addition, since 2018 the industry has improved its practices regarding FERPA compliance as seen by Q1 and Q3 increasing by roughly 10%, meaning 50% of the industry improved their FERPA scores roughly an average of 10%. Lastly, because the

industry has improved its FERPA compliance-related practices since 2018, outliers that are denoted with circles in 2019 are now considered below the range of industry best practices and should update their terms accordingly.

Student Online Personal Information Protection Act (SOPIPA)

Figure 9 illustrates the statute scores for SOPIPA, which is a California state law with many requirements that includes that the application or service must only use student information for educational purposes and must maintain reasonable security standards and that they are prohibited from using student data for tracking, profiling, or behavioral advertising.[28] Table 6 compares and summarizes the SOPIPA statute score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 6: 2018 vs. 2019 SOPIPA score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	9	38	49	48	60	80
2019	9	46	57	56	69	86

From the analysis of SOPIPA-related questions, we determined a median in 2019 of approximately 57%. This median is lower than expected, given that these applications and services are intended for children and students and a majority of companies disclose qualitatively better practices, indicating they only use student information for the educational purpose of providing the services. However, this lower SOPIPA statute score may be attributable to incorrect assumptions by companies that SOPIPA does not apply to their applications and services because their product is intended for a general or mixed audience and is not primarily used by K–12 students.

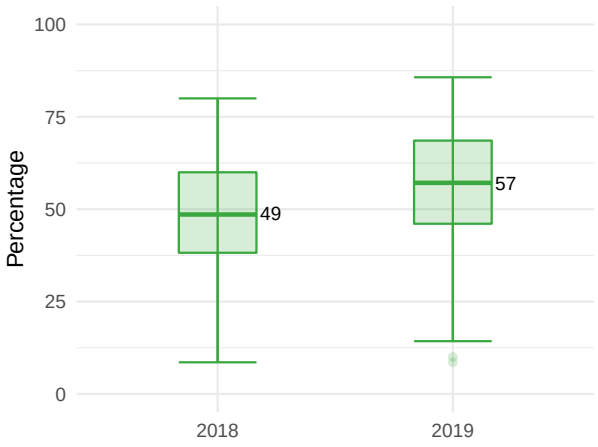


Figure 9: Comparison of SOPIPA scores year over year

Compared to 2018, applications and services evaluated in 2019 indicate a 16% increase in median SOPIPA scores that indicate more transparent and qualitatively better practices regarding the protection of personal information obtained from students. In addition, since 2018, the industry has improved its practices regarding SOPIPA compliance as seen by scores within the second, third, and fourth quartiles increasing by roughly 8%. Lastly, because the industry has improved its SOPIPA compliance-related practices since 2018, outliers that are denoted with circles in 2019 that were within the lower whisker in 2018 are now considered below the range of industry best practices and should update their terms accordingly.

General Data Protection Regulation (GDPR)

Figure 10 illustrates the statute scores for Europe's GDPR, which is an international privacy law that came into effect in 2018 with many reporting and compliance requirements for companies.[29] The law provides European citizens with greater data rights and control over the collection, use, and disclosure of their personal information, but many U.S. companies provide the same privacy protections to all users of their products, and they affect both European and U.S. children and students. Our evaluation questions are based on a framework of universal privacy principles, which means we evaluate concerns that may be addressed in future legislation as well as in existing legislation. As new legislation is passed, we can associate our existing evaluation questions with new legislative requirements. This comprehensive approach allows us to indicate the impact on GDPR statute scores before and after the law came into effect in 2018. Table 7 compares and summarizes the GDPR statute score minimum, maximum, median, mean, Q1 (point between the

[28] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584.

[29] *See* General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 7: 2018 vs. 2019 GDPR score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	16	42	51	51	60	87
2019	18	52	59	60	71	86

From the analysis of GDPR-related questions, which represent approximately 40% of all our questions, we determined a median in 2019 of approximately 59%. This median is lower than expected, given that these applications and services are intended for children and students subject to the GDPR in Europe and intended for children and students in the United States. From the analysis, it would appear that a majority of companies updated their policies in 2018 to disclose qualitatively better practices including that they allow users to exercise their rights to access, review, modify, delete, and export their personal information.

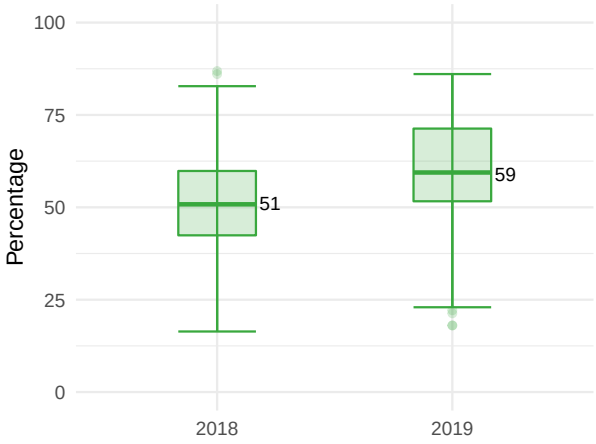


Figure 10: Comparison of GDPR scores year over year

Compared to 2018, applications and services evaluated in 2019 indicate a 15% increase in median GDPR scores that indicate more transparent and qualitatively better practices regarding the collection, use, and disclosure of personal information. In addition, since 2018 the industry has improved its practices regarding GDPR compliance, as seen by the scores within the second and third quartiles increasing by roughly 10%. Lastly, because the industry has improved its GDPR compliance-related practices since 2018, outliers that are denoted with circles in 2019 that were within the lower whisker in 2018 are now considered below the range of industry best practices and should update their terms accordingly.

California Data Breach (Security Breach)

Figure 11 illustrates the statute scores for California's data breach notification statute, which requires the application or service to implement reasonable security practices to protect personal information, and to provide notification to users in the event of a security breach if unencrypted personal information is reasonably believed to have been acquired by an unauthorized person.[30] Table 8 compares and summarizes California's data breach statute score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 8: 2018 vs. 2019 data breach score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	0	25	50	50	75	100
2019	0	25	50	60	100	100

From the analysis of data breach-related questions, we determined a median in 2019 of approximately 50%. This median is lower than expected, given that these applications and services are intended for children and students and that a majority of companies disclose qualitatively better practices and implement reasonable security practices to protect personal information. However, this lower data breach statute score is likely attributable to applications and services that disclose that they notify users in the event of a data breach but do not disclose any additional security practices to protect personal information, such as encryption of personal information in transit and while at rest, or vice versa. Lastly, some companies may have increased their transparency on this statute for compliance purposes when purchasing data breach insurance in 2018, which required that they disclose their data breach notification procedures, including the method of notification and time frame in which to notify users in the event of a data breach.

[30] *See* California Data Breach Notification Requirements, Cal. Civ. Code §§ 1798.29, 1798.82.

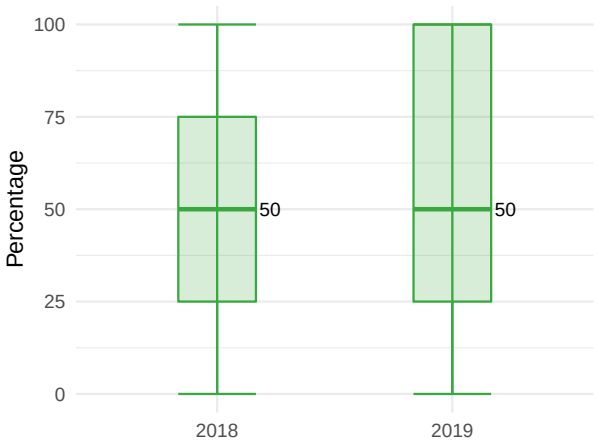


Figure 11: Comparison of California data breach notification requirements (data breach) scores year over year

Compared to 2018, applications and services evaluated in 2019 indicate no change in California data breach median scores but a 16% increase in the mean scores. This trend indicates that companies with low scores in 2018 did not update their policies with more transparent or qualitatively better practices regarding their security practices, but companies with already high scores in 2018 updated their policies and as a result improved their 2019 data breach statute scores. However, Q3 increased to 100 in 2019, indicating at least 25% of the scores in 2019 are at 100%.

California Privacy of Pupil Records (AB 1584)

Figure 12 illustrates the statute scores for California's privacy of pupil records; AB 1584 is a California state law with many requirements that authorizes a local educational agency (LEA) to enter into a third-party contract with an application or service for the collection and use of pupil records.[31] Table 9 compares and summarizes California's privacy of pupil records statute score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 9: 2018 vs. 2019 AB 1584 score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	0	30	42	45	60	100
2019	0	40	60	58	79	100

From the analysis of AB 1584-related questions, we determined a median in 2019 of approximately 60%. Even with this significant increase, the median score is lower than expected, given that these applications and services are intended for children and students and that a majority of companies disclose qualitatively better practices including that collected information will only be used for the educational purpose of providing the service.

However, this lower median score may be the result of companies that enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent requests to access and review that data from eligible students, teachers, and parents. These companies may assume that because the contract discloses that the school, district, or faculty control the deployment of the application or service and administration of student accounts and that they do not also need to disclose those practices in their policies.

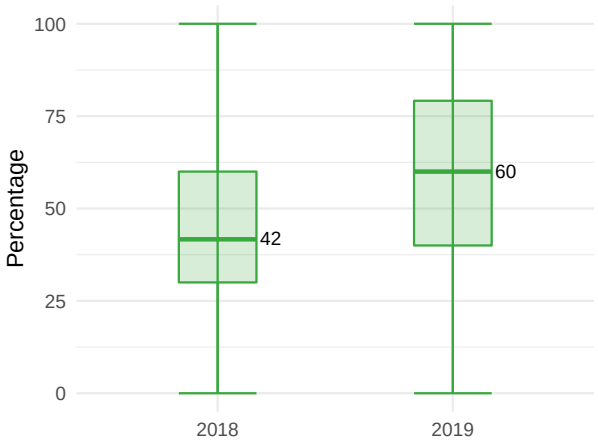


Figure 12: Comparison of California AB 1584: Privacy of Pupil Records scores year over year

Compared to 2018, applications and services evaluated in 2019 indicate a 42% increase in AB 1584 median scores that indicate a significant increase in transparent and qualitatively better practices regarding the protection of students' personal information. In addition, since 2018 the industry has improved its practices regarding contractual compliance with LEAs as seen by scores within the second and third quartiles increasing their median scores by 10% to 19%. Lastly, this increase is not surprising because AB 1584's compliance requirements overlap with many other student data privacy laws such as FERPA and SOPIPA, and we saw similar increases in those respective statute scores.

California Online Privacy Protection Act (CalOPPA)

Figure 13 illustrates the statute scores for CalOPPA, which is a California state law with many requirements, including

[31] *See* California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code §§ 49073-49079.7.

that an application or service that collects personally identifiable information through the internet about individual consumers from California who use or visit its service must: post a privacy policy, identify the categories of personally identifiable information that they collect, identify the categories of third parties they share data with, and provide notice of the effective or revision date of its privacy policy.[32] Table 10 compares and summarizes the CalOPPA statute score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 10: 2018 vs. 2019 CalOPPA score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	27	50	60	59	69	81
2019	31	62	71	68	77	85

From the analysis of CalOPPA-related questions, we determined a median in 2019 of approximately 71%. This median is lower than expected, given that these applications and services are intended for children and students and that a majority of companies disclose qualitatively better practices, including that they post a privacy policy and provide notice of the effective or revision date of its privacy policy. Comparatively, the CalOPPA median is the highest of all the statutory scores analyzed for this report, likely because the requirements of posting a privacy policy, disclosing an effective date, and identification of personal information collected and shared with third parties are basic requirements of a privacy policy.

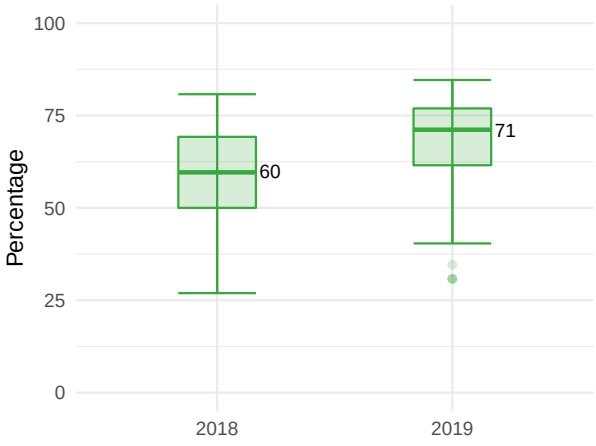


Figure 13: Comparison of California Online Privacy Protection Act (CalOPPA) scores year over year

[32] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §§ 22575-22579.

Compared to 2018, applications and services evaluated in 2019 for the statute of CalOPPA indicate an 18% increase in median scores that indicate more transparent and qualitatively better practices of the minimum requirements of a privacy policy. In addition, since 2018 the industry has significantly improved its practices regarding CalOPPA, as seen by scores within the second and third quartiles increasing by roughly 10%. Lastly, because the industry has significantly improved its CalOPPA compliance-related practices since 2018, outliers that are denoted with circles in 2019 are now considered below the range of industry best practices and should update their terms accordingly.

RESULTS

The 2019 *State of EdTech Privacy Report* should not only be used as a means to inform individuals about the general state of privacy practices in the edech industry, but also as a resource that provides insight into our Evaluation Process. As we look to improve our understanding and communication of our findings to users of varying degrees of privacy awareness, as described in Evaluation Details, we are extremely critical of any adjustments to our evaluation process to ensure we are both reporting data accurately and that we are not providing a false sense of security. This is an extremely challenging proposition, especially in a field as nuanced as privacy and given the extremely disparate concerns of various audiences. While there are certainly issues of bias in any longitudinal study, we have aimed to be consistent as well as transparent, as described in our Methodology section, where we note any known shortcomings in our evaluation process.

Interpreting results certainly provides an opportunity to misunderstand what the data is informing us about, as well as overinflating shifts and trends in industry behavior. Evaluations that receive our full, rather than basic, evaluation do experience a selection bias in several ways:

1. They are filtered by those products that are experiencing wide industry use and adoption;
2. They are filtered by those products that potentially have access to more sensitive data; and
3. They tend to limit low-quality products that may not have done due diligence with respect to informing users of their respective privacy practices.

As such, it should be expected that our analysis likely overestimates industry practices in a positive direction, and it would be expected that the industry's privacy practices are less transparent and qualitatively worse than the filtered selection of products that receive a full evaluation from the Common Sense Privacy Program.

Additional challenges presented are posed by increasing the number of products evaluated. In 2018, the *State of EdTech Report* included 100 evaluations. In 2019, we have included an additional 55 products, and removed the five products that were discontinued, for a total of 150 products evaluated. This is a 50% year-over-year increase in the number of evaluations being considered in the state of edtech analysis. Given such a large increase in the number of products evaluated, some of our findings may indicate an unintended selection bias on our part as well as general shifts in the industry. We have done our best to ensure that our selection process has remained consistent year over year, but inevitably some of our results will likely be an indication of unintended biases reflected in the results, which we will continue to analyze in our research. That said, we see several areas that remain consistent as well as several areas where industry standard norms appear to be shifting.

In general, box plots and bar charts are used throughout the report to compare 2018 and 2019 data. All other graphs will tend to analyze 2019 data only to ensure we are assessing trends only where it is appropriate. Analysis that only includes 2019 data is intended to aid in the future direction of the Privacy Program, including our ongoing efforts to improve messaging, while providing a larger percentage of evaluated products.

Score Distributions

The following score distributions illustrate the overall scores for both basic and full scores for 150 popular edtech applications and services. Each comparison chart below is a box plot and described further in the Procedural Changes section.

Basic Scores

Among the applications and services evaluated, table 11 illustrates basic score statistics. From the analysis of 34 basic evaluation questions, we determined a median in 2019 of approximately 65%. This median is lower than expected, given that these applications and services are intended for children and students. The basic evaluation questions were selected to be a representative subset of our full evaluation question set, including all the related questions in the Evaluation Tiers section, which are a varying and in some cases nonrepresentative subset of concern questions as seen in the Privacy Concerns section. For example, basic evaluation questions include a subset of questions from all nine privacy concerns, and, to a varying degree of quality, a basic score may serve as a reliable prediction of a full evaluation score, as discussed in the Regression Analysis section. Lastly, the median for basic scores is higher, and the minimum and maximum for basic scores is a wider range than as described in the Full Scores section below.

Table 11: 2018 vs. 2019 Basic Score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	9	44	56	55	68	93
2019	9	53	65	64	79	94

Compared to 2018, applications and services in 2019 indicate a 16% increase in overall basic median scores that indicate more transparent and qualitatively better practices across a wide range of privacy practices. In addition, since 2018, the industry has improved with greater transparency and better practices across all basic questions, as seen by scores within the second and third quartiles increasing by roughly 11%. Lastly, because the industry has significantly improved its basic privacy practices since 2018 across all concerns, outliers denoted with circles in 2019 are now considered below the range of basic industry best practices and should update their terms to reflect the better practices the industry has adopted since last year.

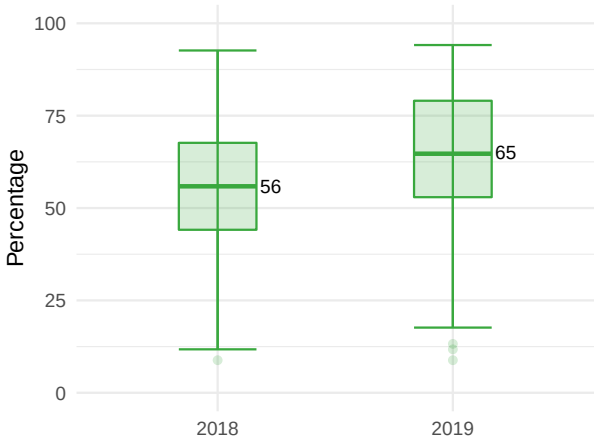


Figure 14: Comparison of basic scores year over year

Full Scores

Among the applications and services evaluated, table 12 illustrates full score statistics. From the analysis of 150 full evaluation questions, we determined a median in 2019 of approximately 52%. This median is lower than expected, given that these applications and services are intended for children and students. Similar to basic evaluation questions, full evaluation questions are represented on all tiers. Additionally, 10 full evaluation questions compose each of the respective nine concerns. Lastly, the median for full scores is lower, and the minimum and maximum for basic scores is a smaller range than Basic Scores. This is likely because there are more than four times as many full evaluation questions and it is difficult for companies to address the wider range of privacy and security practices.

Table 12: 2018 vs. 2019 Full Score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	13	37	45	44	52	80
2019	13	45	52	52	61	77

Compared to 2018, applications and services in 2019 indicate a 15% increase in full median scores that indicate more transparent and qualitatively better practices across a wide range of privacy practices. Interestingly, our findings indicate a similar percent increase in the median of basic scores, which likely indicates that companies updated their policies with greater transparency and qualitatively better practices for those concerns covered by our basic evaluation questions. In addition, since 2018, the industry has improved with greater transparency and better practices across all concerns as seen by scores within the second and third quartiles increasing by 8%. Lastly, because the industry has significantly improved its basic privacy practices since 2018, outliers that are denoted with circles in 2019 are now considered below the range of basic industry best practices and should update their terms to reflect the better practices the industry has adopted since last year.

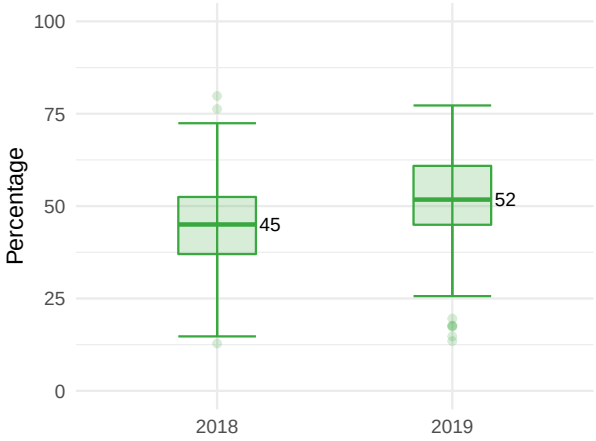


Figure 15: Comparison of full scores year over year

Regression Analysis

For all of the graphs comparing a full score to a basic score, the intent is to identify those concern, statutory, and comprehensive scores where the basic score is a reliable indicator of a full score. From our analysis in all cases, regardless of reliability, basic scores tend to overestimate the respective full score. This makes sense as high-priority details or concerns will tend to be better and more explicitly covered in privacy policies, whereas more nuanced or specialized concerns will tend to have fewer policies addressing those concerns industry-wide. We consistently use the full score on the y-axis and the basic score on the x-axis, and each dot represents one evaluation. The line that is graphed is a generalized linear model with the blue shaded area indicating the 95% prediction interval. In other words, the line and blue area surrounding it indicate that given a basic score, at that point on the line, we would expect 95% of the corresponding full scores to fall within the shaded blue area. The caption of each graph also indicates the r^2 value, which is an indication of how well our linear model explains the variance in data. For the purposes of our basic to full score comparisons, $r^2 \geq 0.7$, and a prediction interval range less than 30 is considered a "reliable predictor." However, when $r^2 \leq 0.7$, the linear model does not adequately describe the variance in full scores, and when prediction interval range is greater than 30, the prediction interval is too large for a basic score to provide any meaningful or reliable insight into a potential full score and is considered an "unreliable predictor" for our purposes. The variance in the prediction interval size is likely a reflection of several details:

1. How representative are the basic evaluation questions for the given facet of scoring?
2. How complicated is the given privacy concern?
3. Are policies generally only covering the basic subset of questions? In this scenario the full evaluation questions may not be covered in the policies, and as a result the only information we have is represented in the basic questions.
4. Are the policies covering all of the questions?
5. How variable are vendor responses relative to other responses in the same concern? This might explain why we see that Ads & Tracking and Data Sold basic scores are extremely poor predictors of a full score. Perhaps vendors' policies are more transparent with the questions in these concerns and there is more variability in vendor responses across the full set of questions as compared to just the basic questions.

We expect to see the comprehensive basic to full score regression to be a very reliable predictor, as the basic evaluation questions were previously selected as a representative sample of the full evaluation question set. However, we expect that some of our concern breakdowns, especially those not well represented in our basic evaluation questions, will not be as predictive given the narrow coverage in our basic evaluation questions. To determine which questions should be part of our basic evaluation, we relied on our existing expertise, feedback from our District Privacy Consortium of schools and districts, and known privacy concerns of the general public, as well as extensive data analysis to identify which question responses in our existing evaluations were heavily correlated indicating they may provide minimal additional statistical information. This is our second year of col-

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

lecting data, and our findings confirm our previous decisions and continue to provide insight into what a full evaluation might surface given a basic evaluation. It should be noted, however, that this does not mean a basic evaluation is sufficient. In many instances, especially when making decisions on behalf of other people, the implicit and explicit details do matter. So while a basic score may be a good predictor of a full score in some cases, it may not be sufficient to make a completely informed decision. There is also concern that over time the basic evaluation questions will provide additional incentive for a product to be just transparent enough to earn a high basic score but fail to address the larger picture or more nuanced Privacy Concerns as covered in our full evaluations.

Basic and Full Score Comparison

Figure 33 illustrates a comparison between the overall basic score and full score for all the applications or services evaluated for this report. Our findings indicate the basic score is a reliable predictor of the full score, which is expected because the 34 basic questions are a subset of the 156 full evaluation questions. The prediction interval suggests a range around the linear regression of ± 11 points and an r^2 value greater than 0.7. Lastly, it appears the basic score overpredicts the full score with a range from approximately 12% to 25%.

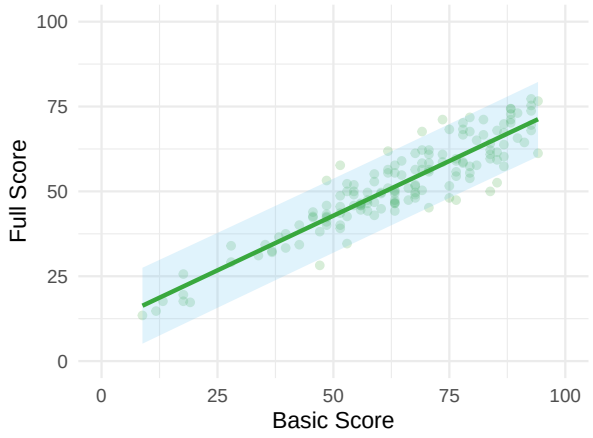


Figure 16: Comparison of 2019 comprehensive Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 11 + 0.64(x) \pm 11$, and $r^2 = 0.833$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

Tiers and Full Score Comparison

Figure 17 illustrates the tiers and full score statistics among the 150 popular edtech applications and services evaluated. Table 13 summarizes the tiers and their respective full score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 13: Tier score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
Not Recommended	13	15	17	22	26	34
Use with Caution	15	43	49	48	56	71
Use Responsibly	45	58	64	63	70	77

From the analysis of the tiers and their respective full scores for all the applications or services evaluated in 2019, as described in the Evaluation Tiers section, we determined a median of the blue Use Responsibly tier of approximately 64%. In addition, we determined a median of the orange Use with Caution tier of approximately 49% and a median of the red Not Recommended tier of approximately 17%.

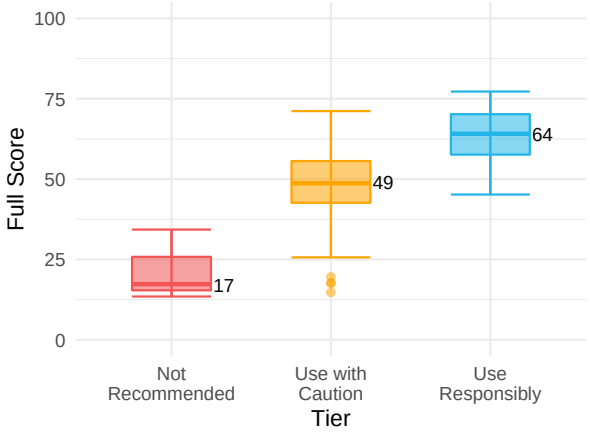


Figure 17: Distribution of 2019 scores relative to their respective tiers

The low Not Recommended tier score is expected because the minimum score will always skew to 0, given that many products in the Not Recommended tier do not make a privacy policy available to users and therefore do not earn any points in our evaluation. In addition, the Not Recommended tier maximum score is within the first quartile of the Use with Caution tier, which is expected given that many of the products in this low score range only disclose a handful of privacy and security issues in their policies. However, what differentiates Not Recommended products in the fourth quartile from products in the Use with Caution first quartile is that Not Recommended products do not use reasonable security practices such as encryption to protect data collected from children or students, but may provide other privacy protections.

However, the Use Responsibly median score is lower than expected, given that these applications and services are intended to be used by children and students. Companies in this tier are required to disclose qualitatively better practices including that they do not sell data to third parties or engage in behavioral ads, tracking, or third-party marketing with children and students. This lower score is likely the result of companies focusing exclusively on disclosing qualitatively better practices to ensure they are not in the Use with Caution tier, but failing to disclose additional privacy and security practices resulting in a lower overall score. Interestingly, the Use Responsibly lower quartile is roughly equal to the Use with Caution upper quartile, and the Use Responsibly minimum is within the Use with Caution second quartile. Therefore, these findings suggest there are many applications and services with a Use Responsibly tier designation that disclose qualitatively better practices but have less robust policies and earn the same full score as many products with a Use with Caution tier. Also, because the industry has improved its tier-related practices since 2018, outliers that are denoted with circles are now considered below the range of industry best practices and should update their terms accordingly.

Moreover, approximately 75% of the Use with Caution tier full scores fall within the range of scores earned by products in the tier Use Responsibly. This overlap of the two tiers suggests that the privacy practices of the edtech industry have matured to the extent that our evaluation process should raise the requirements for products to earn our top Use Responsibly tier. Also, the full score overlap between the two tiers indicates that additional information is required for parents and educators to make an informed decision when presented with two products with the same full score but different tiers. As described in our Privcay Concerns section, our evaluation process also provides additional details about a product beyond a tier and full score. Concern scores help parents and educators compare products based on the issues that matter to them, such as data collection, data safety, data security, and parental consent.

Data Collection Comparison

Figure 18 illustrates a comparison of full evaluation Data Collection concern scores to basic evaluation Data Collection concern scores among all applications and services evaluated. This analysis shows that the basic concern of Data Collection, with only 20% representation of a full concern, is unsurprisingly an unreliable predictor of a full Data Collection concern score with 10 questions. The prediction interval suggests a range around the linear regression of ± 23 points and r^2 value less than 0.7. However, this is expected given the nuance and wide range of full Data Collection concern questions and the basic evaluation questions only including two of the Data Collection questions.

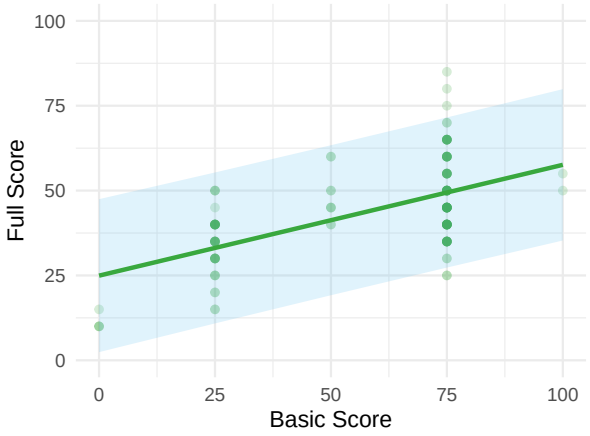


Figure 18: Comparison of 2019 Data Collection Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 25 + 0.33(x) \pm 23$, and $r^2 = 0.333$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Data Sharing Comparison

Figure 19 illustrates a comparison of full evaluation Data Sharing concern scores and basic evaluation Data Sharing concern scores among all applications and services evaluated. This analysis shows that the basic concern of Data Sharing with 40% representation of a full concern is a reliable predictor of a full Data Collection concern score with 10 questions. In addition, there is expected variance between the basic and full concern scores at several points, which indicates that the basic concern score both underpredicts and overpredicts a full concern score. The prediction interval suggests a range around the linear regression of ± 14 points and an r^2 value greater than 0.7. This is a strong indication that the basic question selection is representative of data sharing practices across a wide range of nuanced concerns.

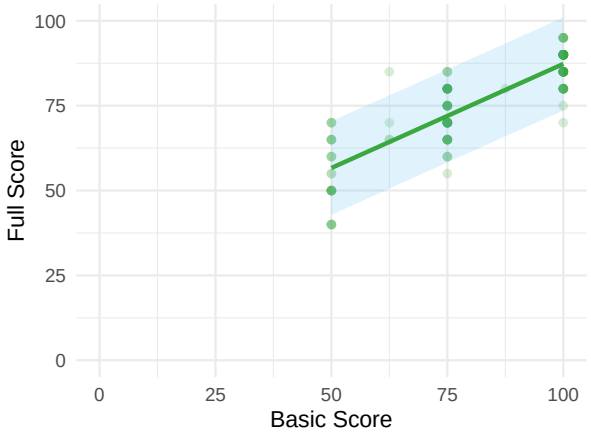


Figure 19: Comparison of 2019 Data Sharing Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 26 + 0.61(x) \pm 14$, and $r^2 = 0.727$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

Data Security Comparison

Figure 20 illustrates a comparison of full evaluation Data Security concern scores and basic evaluation Data Security concern scores among all applications and services evaluated. This analysis shows that the basic concern of Data Security with a high representation of 60% of a full concern is a reliable predictor of a full Data Collection concern score with 10 questions. The prediction interval suggests a range around the linear regression of ± 18 points and an r^2 value greater than 0.7. This is a strong indication that the basic question selection is representative of data security practices across a wide range of nuanced concerns.

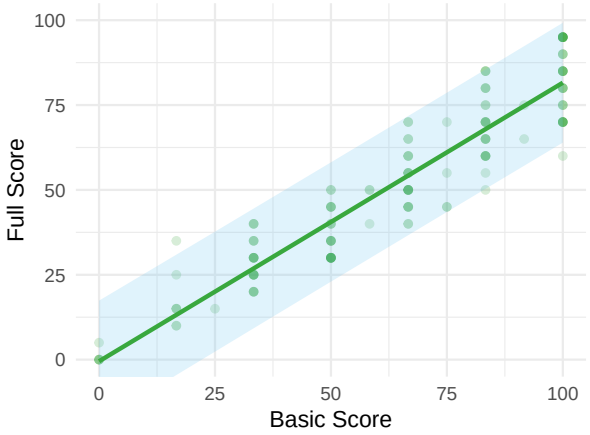


Figure 20: Comparison of 2019 Data Security Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = -0.49 + 0.82(x) \pm 18$, and $r^2 = 0.873$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

Data Rights Comparison

Figure 21 illustrates a comparison of full evaluation Data Rights concern scores and basic evaluation Data Rights concern scores among all applications and services evaluated. This analysis shows that the basic concern of Data Rights with 40% representation of a full concern is an unreliable predictor of a full Data Collection concern score with 10 questions. The prediction interval suggests a range around the linear regression of +/-25 points, which is too large to infer a reliable prediction of what a full score might be. However, this large variance is expected given the nuance and wide range of Data Rights concern questions.

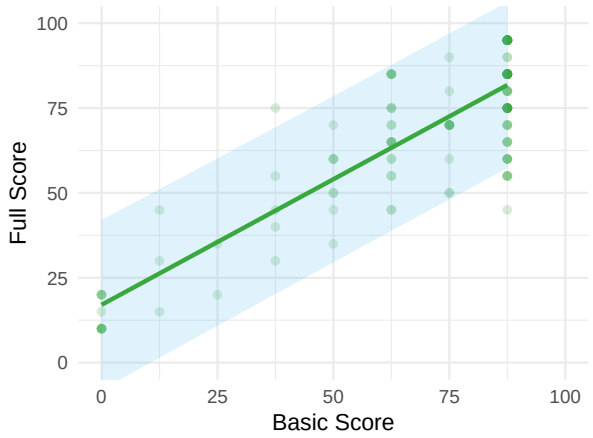


Figure 21: Comparison of 2019 Data Rights Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 17 + 0.74(x) \pm 25$, and $r^2 = 0.718$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

Data Sold Comparison

Figure 22 illustrates a comparison of full evaluation Data Sold concern scores and basic evaluation Data Sold concern scores among all applications and services evaluated. This analysis shows that the basic concern of Data Sold with only 20% representation of a full concern is an extremely poor predictor of a full Data Collection concern score with 10 questions. The prediction interval suggests a range around the linear regression of ± 33 points and an r^2 value less than 0.7. However, this huge variance is expected given the nuance and wide range of full Data Sold concern questions.

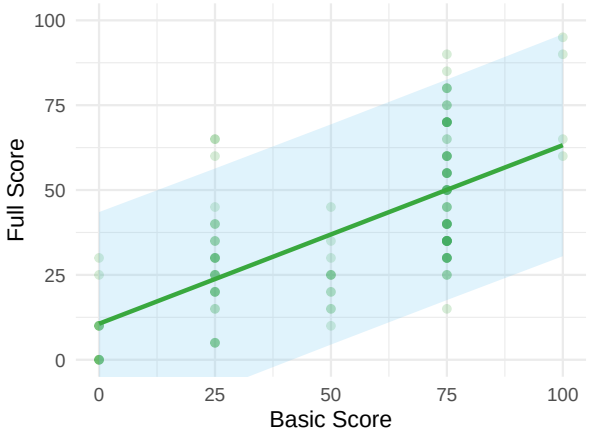


Figure 22: Comparison of 2019 Data Sold Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 11 + 0.53(x) \pm 33$, and $r^2 = 0.438$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Data Safety Comparison

Figure 23 illustrates a comparison of full evaluation Data Safety concern scores and basic evaluation Data Safety concern scores among all applications and services evaluated. This analysis shows that the basic concern of Data Safety with 40% representation of a full concern is an unreliable predictor of a full Data Safety concern score with 10 questions. The prediction interval suggests a range around the linear regression of +/-20 points, which is too large to infer a reliable prediction of what a full score might be. However, this large variance is expected given the nuance and wide range of full Data Safety concern questions.

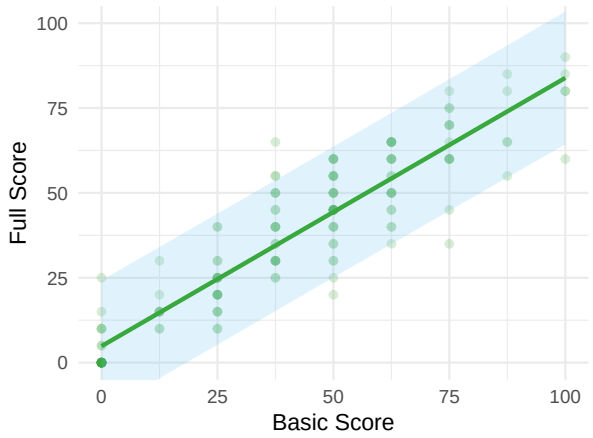


Figure 23: Comparison of 2019 Data Safety Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 4.9 + 0.79(x) \pm 20$, and $r^2 = 0.839$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

Ads and Tracking Comparison

Figure 24 illustrates a comparison of full evaluation Ads & Tracking concern scores and basic evaluation Ads & Tracking concern scores among all applications and services evaluated. This analysis shows that the basic concern of Ads & Tracking with 60% representation of a full concern is an unreliable predictor of a full Ads & Tracking concern score with 10 questions. The prediction interval suggests a range around the linear regression of +/-20 points, which is too large to infer a reliable prediction of what a full score might be. However, this large variance is expected given the nuance and wide range of full Ads & Tracking concern questions.

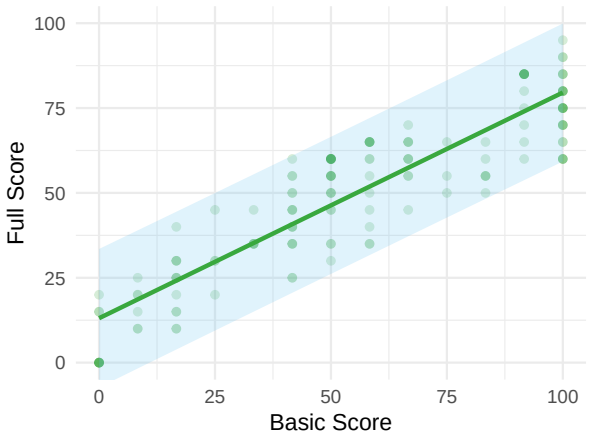


Figure 24: Comparison of 2019 Ads & Tracking Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 13 + 0.66(x) \pm 20$, and $r^2 = 0.815$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

Parental Consent Comparison

Figure 25 illustrates a comparison of full evaluation Parental Consent concern scores and basic evaluation Parental Consent concern scores among all applications and services evaluated. This analysis shows that the basic concern of Parental Consent with only 30% representation of a full concern is an unreliable predictor of a full Parental Consent concern score with 10 questions. The prediction interval suggests a range around the linear regression of +/-26 points, which is too large to infer a reliable prediction of what a full score might be. However, this large variance is expected given the nuance and wide range of full Parental Consent concern questions.

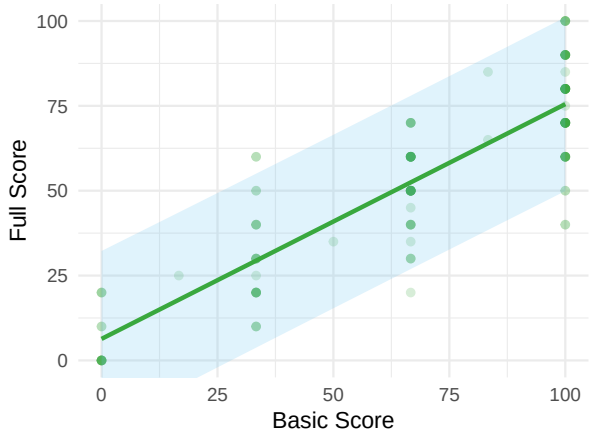


Figure 25: Comparison of 2019 Parental Consent Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 6.3 + 0.69(x) \pm 26$, and $r^2 = 0.758$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

School Purpose Comparison

Figure 26 illustrates a comparison of full evaluation School Purpose concern scores and basic evaluation School Purpose concern scores among all applications and services evaluated. This analysis shows that the basic concern of School Purpose with only 20% representation of a full concern is an unreliable predictor of a full School Purpose concern score with 10 questions. The prediction interval suggests a range around the linear regression of +/-20 points, which is too large to infer a reliable prediction of what a full score might be. However, this large variance is expected given the nuance and wide range of full School Purpose concern questions.

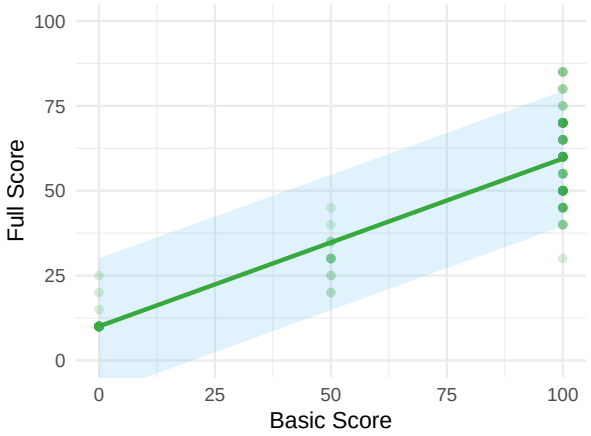


Figure 26: Comparison of 2019 School Purpose Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 10 + 0.49(x) \pm 20$, and $r^2 = 0.812$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Statute Score Comparisons

The following statute score comparisons are calculated against the respective number of questions in each statute breakdown. Each statute or regulation is associated with one or more evaluation questions. As described in the Statute Scores section, we can calculate scores for each statute or regulation using only those questions associated with the statute or regulation. Each specific statute or legislations's score serves as an indirect proxy indicating the likelihood of the application or service satisfying all of its compliance obligations. In this section, we analyze the relationship between the basic evaluation questions related to a specific statute and the full evaluation questions related to that same statute to determine whether, given a basic score, we can reliably infer what a full score for that application or service might be.

COPPA Comparison

Figure 27 illustrates a comparison of full evaluation COPPA statute scores to basic evaluation COPPA statute scores among all applications and services evaluated.[33] This analysis shows that the basic statute coverage of COPPA-related compliance questions is a reliable predictor of the full COPPA statute score. In addition, the prediction interval suggests a range around the linear regression of ± 11 points and an r^2 value greater than 0.7. We expect this prediction to be reliable given our findings of the overall basic score and full score and the COPPA-related questions composing nearly 50% of our full evaluation questions.

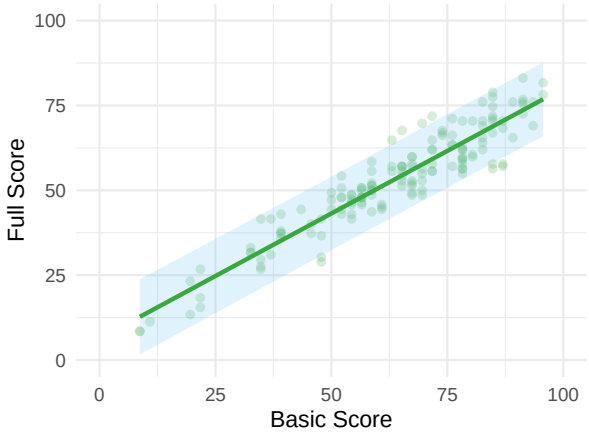


Figure 27: Comparison of 2019 COPPA Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 6.3 + 0.74(x) \pm 11$, and $r^2 = 0.873$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

FERPA Comparison

Figure 28 illustrates a comparison of full evaluation FERPA statute scores and basic evaluation FERPA statute scores among all applications and services evaluated.[34] This analysis shows that the basic statute coverage of FERPA-related compliance questions is a reliable predictor of the full FERPA statute score. The prediction interval suggests a range around the linear regression of ± 15 points and r^2 value greater than 0.7. This is a strong indication that the basic question selection is representative of FERPA compliance, comprising roughly 25% of our full evaluation questions, across a wide range of nuanced concerns.

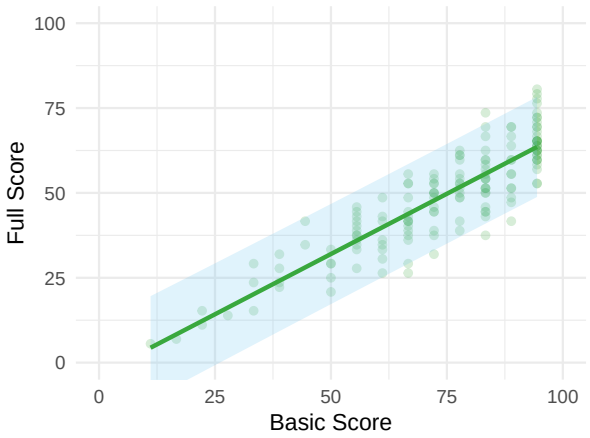


Figure 28: Comparison of 2019 FERPA Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = -3.5 + 0.71(x) \pm 15$, and $r^2 = 0.771$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

[33] *See* Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501-6508.

[34] *See* Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, 34 CFR Part 99.

SOPIPA Comparison

Figure 29 illustrates a comparison of full evaluation SOPIPA statute scores and basic evaluation SOPIPA statute scores among all applications and services evaluated.[35] This analysis shows that the basic statute coverage of SOPIPA-related compliance questions is a reliable predictor of the full SOPIPA statute score. In addition, the prediction interval suggests a range around the linear regression of ± 12 points and an r^2 value greater than 0.7. This is a strong indication that the basic question selection is representative of SOPIPA compliance, comprising roughly 35% of our full evaluation questions, across a wide range of nuanced concerns.

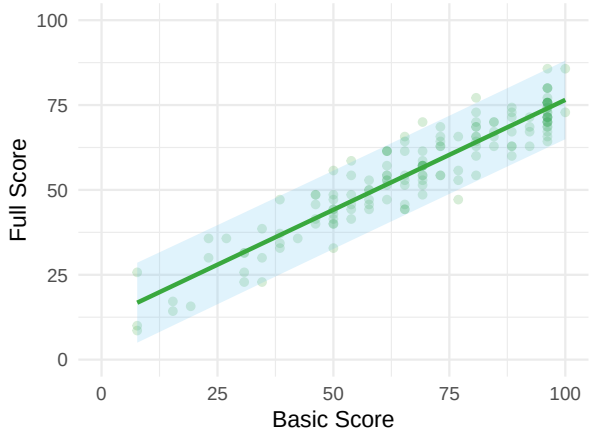


Figure 29: Comparison of 2019 SOPIPA Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 12 + 0.65(x) \pm 12$, and $r^2 = 0.871$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

GDPR Comparison

Figure 30 illustrates a comparison of full evaluation GDPR statute scores and basic evaluation GDPR statute scores among all applications and services evaluated.[36] This analysis shows that the basic statute coverage of GDPR-related compliance questions is a reliable predictor of the full GDPR statute score. The prediction interval suggests a range around the linear regression of ± 15 points and an r^2 value greater than 0.7. This is a strong indication that the basic question selection is representative of GDPR compliance, comprising roughly 25% of our full evaluation questions, across a wide range of nuanced concerns.

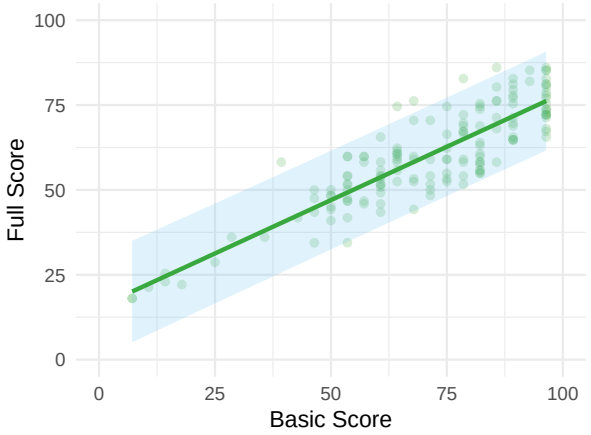


Figure 30: Comparison of 2019 GDPR Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 16 + 0.63(x) \pm 15$, and $r^2 = 0.757$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

[35] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584.

[36] *See* General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Data Breach Comparison

Figure 31 illustrates a comparison of full evaluation California data breach statute scores and basic evaluation California data breach statute scores among all applications and services evaluated.[37] This analysis shows that the basic statute coverage of data breach-related compliance questions is a perfect predictor of the full data breach statute scores, because all full evaluation data breach statute questions are represented in the basic evaluation questions. This analysis is included for completeness and unsurprisingly shows a perfect linear regression and an r^2 value of 1, which is expected because all data breach-related questions are represented in both full and basic statute scores.

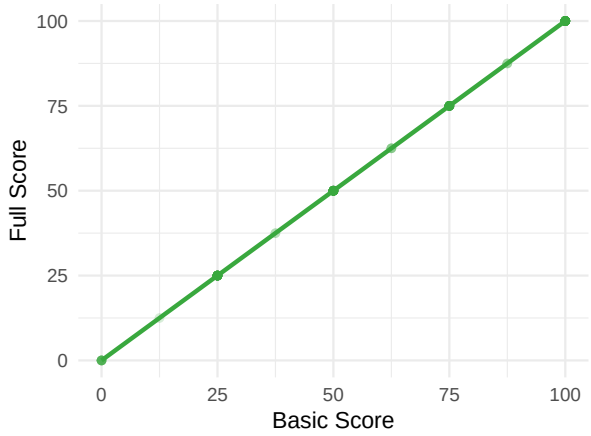


Figure 31: Comparison of 2019 Data Breach Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = x$, and $r^2 = 1$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

Privacy of Pupil Records Comparison

Figure 32 illustrates a comparison of full evaluation Privacy of Pupil Records (AB 1584) statute scores and basic evaluation AB 1584 statute scores among all applications and services evaluated.[38] This analysis shows that the basic statute coverage of AB 1584-related compliance questions is an unreliable predictor of the full AB 1584 statute score. The prediction interval suggests a range around the linear regression of +/-33 points, which is too large to infer a reliable prediction of what a full score might be. However, this large variance is not surprising given that the basic questions only include 20% of the wide-ranging questions related to AB 1584.

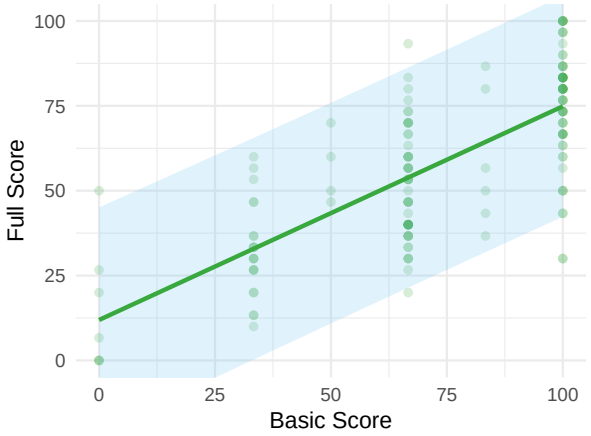


Figure 32: Comparison of 2019 AB 1584 Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 12 + 0.63(x) \pm 33$, and $r^2 = 0.546$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

[37] *See* California Data Breach Notification Requirements, Cal. Civ. Code §§ 1798.29, 1798.82.

[38] *See* California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code §§ 49073-49079.7.

CalOPPA Comparison

Figure 33 illustrates a comparison of full evaluation CalOPPA statute scores and basic evaluation CalOPPA statute scores among all applications and services evaluated.[39] This analysis shows that the basic statute coverage of CalOPPA-related compliance questions is a reliable predictor of the full CalOPPA statute score. The prediction interval suggests a range around the linear regression of ± 13 points and an r^2 value greater than 0.7. This is a strong indication that the basic question selection is representative of CalOPPA compliance, comprising roughly 25% of our full evaluation questions, across a wide range of nuanced concerns.

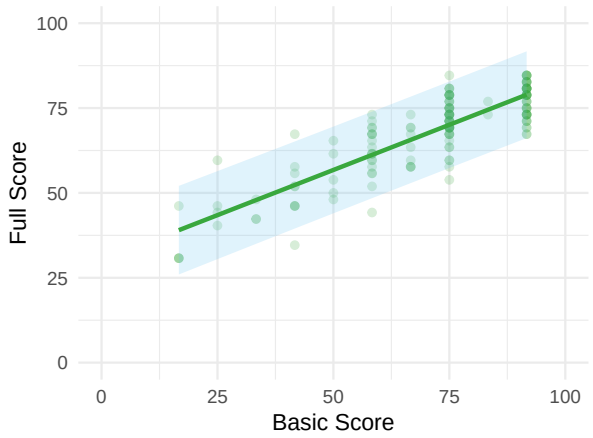


Figure 33: Comparison of 2019 CalOPPA Basic Scores and Full Scores. The green line represents the linear regression defined by the equation $y = 30 + 0.53(x) \pm 13$, and $r^2 = 0.729$, where x is the Basic Score and y is the predicted Full Score. The blue shaded areas indicate the 95% prediction interval where we would expect 95% of the Full Scores to be given a specific Basic Score.

PRIVACY CONCERNS

The privacy evaluation summarize the policies of an application or service into concerns based on a subset of evaluation questions that can be used to quickly identify the practices of a vendor's policies. These concerns are composed of evaluation questions that can be used to calculate scores relative to that concern.[40] The privacy evaluation concerns are composed of both basic and full questions. As such, a basic concern is a subset of a full concern and identifies several critical evaluation questions for a quick comparison between products. A full concern provides a more comprehensive analysis and understanding of an application or service's policies with respect to the specific concern. The basic and full evaluation concerns are organized by two-word question descriptions used to provide a general understanding of the topics covered by each concern. Each concern has its own concern score, which is calculated as a percentage given the number of questions in each concern.

As discussed in the Evaluation Scores section, the scoring methodology for the concerns is the same as the methodology used for the statute scoring and the overall scoring. Table 14 summarizes our findings of the minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 14: 2019 concern score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
Data Collection	10	35	45	44	50	85
Data Sharing	40	70	80	77	85	95
Data Security	0	31	50	53	70	95
Data Rights	10	60	75	69	85	95
Data Sold	0	25	35	40	55	95
Data Safety	0	15	40	36	55	90
Ads & Tracking	0	35	55	50	65	95
Parental Consent	0	40	60	54	70	100
School Purpose	10	26	50	46	65	85

The concerns help provide focused understanding about the different privacy-, security-, safety-, and compliance-related issues that compose a particular concern for an application or service. The concerns ultimately provide parents and teachers with more relevant information to make a more informed decision about whether to use a particular application or service based on the concerns that matter most for their kids and students.

[39] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §§ 22575-22579.

[40] Common Sense Media, *Privacy Questions organized by Concern*, Privacy Program, https://www.commonsense.org/education/privacy/questions/concerns.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Full: Data Collection

Evaluating data collection takes into consideration the best practices of limiting the type and amount of personal information collected from a user to only the information needed to provide the application or service.

Data Collection Scores

Figure 34 illustrates the Data Collection scores among all applications and services evaluated. Table 15 compares and summarizes the Data Collection concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 15: 2018 vs. 2019 Data Collection score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	10	30	40	38	45	65
2019	10	35	45	44	50	85

From the analysis of the 10 questions in the Data Collection concern, we determined a median in 2019 of approximately 45%. This median is lower than expected, given that these applications and services are intended for children and students and that a majority of companies disclose qualitatively better practices, including that they limit the collection of personal information from children.

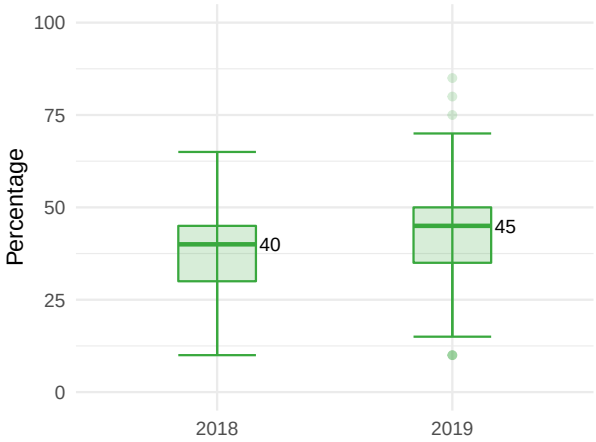


Figure 34: Comparison of Data Collection scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of Data Collection indicate a 12% increase in median scores that indicate more transparent and qualitatively better practices with respect to the collection of personal information. Lastly, because the industry has significantly improved its Data Collection practices since 2018, there are now outliers that are denoted with circles in 2019 in both the positive and negative direction. Those outliers above the upper whisker are exceeding industry norms and providing more clarity and better practices. Additionally, since industry norms have improved, some applications and services are now providing a level of detail below industry norms and their policies should be updated to address these shortcomings. Hopefully the positive outliers indicate a trend for better clarity related to the Data Collection concern, and in 2020 we will see more policies updating their terms to address shifting legislative requirements and user concerns.

Collect PII

Among the applications and services we evaluated in 2019, approximately 3% disclosed a qualitatively better response that they do not collect personally identifiable information (PII). However, our analysis indicates that approximately 2% of applications and services evaluated were unclear on this issue. In other words, our analysis indicates that approximately 95% of applications and services evaluated disclosed that they collected PII.

This qualitatively worse finding is likely the result of applications and services collecting personal information from children and students in order to provide the services. Although not inherently a bad 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 create an unnecessary risk of the information being inappropriately 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.[41,42,43,44,45] For the 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 as described in the Collection Limitation section.

41 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.6(a)(2).
42 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1.
43 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22577(a)(1)-(6).
44 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(o)(1).
45 General Data Protection Regulation (GDPR), Definitions, Art. 4(1).

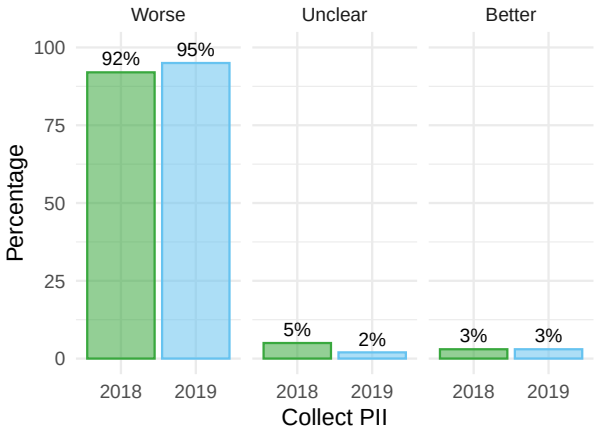


Figure 35: Do the policies clearly indicate whether or not the vendor collects personally identifiable information (PII)?

Compared to 2018, applications and services evaluated in 2019 indicate an additional 3% now collect PII. This negative trend is likely the result of applications and services clarifying their data collection practices regarding the collection of personal information. However, this trend is not unexpected since, as applications and services improve and provide more robust features, they often require the collection of more personal information to provide those features. From our analysis, it appears there is an approximately 64% higher occurrence in the disclosure of qualitatively better practices for the concern of Collection Limitation, which mitigates some of the risks posed by collecting personal information from children and students by only collecting the minimum amount of information from children and students required to provide the service.

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, 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. Therefore, it is recommended that the practice of collecting personal information be mitigated to some extent, as explained in our later analysis of Collection Limitation.

PII Categories

Among the applications and services we evaluated, approximately 92% disclosed that they have listed or described the types of personally identifiable information (PII) that they may or will collect. However, our analysis indicates that approximately 8% of applications and services evaluated did not clearly indicate what types of PII their product would collect. Accordingly, disclosing the types or categories of personal information collected from children and students provides more information about what data is actually collected from the application or service and how that data could be used or shared with third parties. This high percentage of transparent responses is likely because the requirement to disclose the categories of personal information collected is a basic principle of a company's privacy policy and compliance requirement.[46,47,48,49]

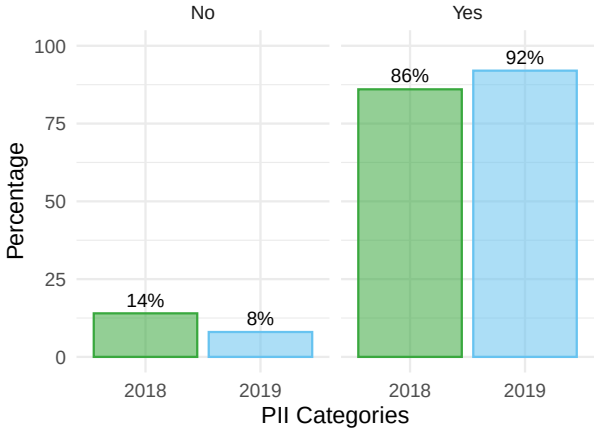


Figure 36: Do the policies clearly indicate what categories of personally identifiable information are collected by the product?

Compared to 2018, applications and services evaluated in 2019 indicate that an additional 6% of companies disclose what types of PII the vendors may collect from the products covered by these policies. This positive trend is likely the result of increased education and understanding by companies about the purposes of privacy policies and that indicating which types of PII they collect is among the most fundamental elements of the policy. While the percentages on this issue are close to approaching industry-wide disclosure, some applications and services need to provide greater transparency on this issue, because these products are among the 150 most popular educational technology products, and although there is a significant percentage of applications and services that disclose they are intended for children and students, some still do not also disclose what types of PII they use.

46 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(1).

47 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part312.6(a)(1).

48 California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100(a)-(b), 1798.140(o)(1)(B).

49 General Data Protection Regulation (GDPR), Art. 14(1)(d), 15(1)(b). Collection Limitation

Collection Limitation

Among the applications or services we evaluated, approximately 67% disclosed a qualitatively better response that they limit the collection or use of information to only data that is specifically required to use the application or service. However, our analysis indicates that approximately 29% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 4% of applications and services evaluated do not limit the collection or use of information to only data that is specifically required to use the application or service.[50,51]

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. This qualitatively worse finding is likely the result of a lack of understanding of best practices for data collection, including data minimization and limiting the data collected to that which is necessary for using the product. In many cases, if a product can collect data, it will collect data, regardless of whether it is necessary or even useful for the product's functionality. Further, some companies allow their products to collect and store data that they are not using currently to provide the service but "may" use in some capacity at a later time. It may be tempting for a company to collect as much data as possible about children or students to create huge databases of personal information, but this practice is considered a worse practice in our evaluation process because large unnecessary databases of personal information could later be compromised in a data breach, as discussed in the Data Breach section, and/or by misuse by current or future custodians of the data.

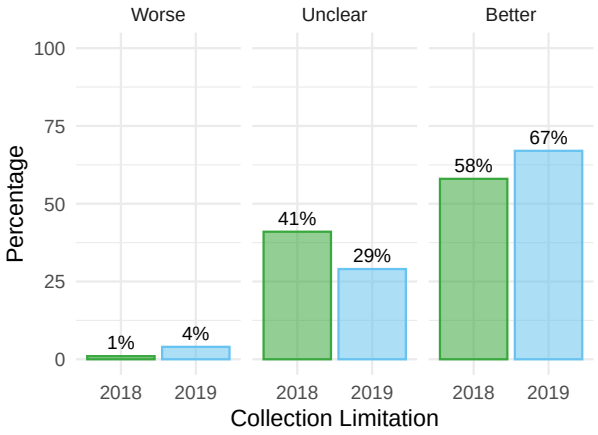


Figure 37: Do the policies clearly indicate whether or not the vendor limits the collection or use of information to only data that is specifically required for the product?

Compared to 2018, applications and services evaluated in 2019 indicate an additional 9% in qualitatively better practices in that they limit the collection or use of information to only data that is specifically required to use the application or service. This positive trend may be the result of an increased understanding of the risks of legal prosecution and data breach liability costs associated with the over-collection of personal information. Of course, if a high percentage of companies is collecting personal information, as discussed in the Collect PII section, a much higher percentage of companies should be indicating that they are limiting collection of PII to the necessary information in order to operate their product. Therefore, applications and services need to disclose better practices on this issue, because these products are among the 150 most popular educational technology products, and although there is a significant percentage of applications and services that disclose they are intended for children and students, they do not also indicate that they limit data collection from kids.

Geolocation Data

Among the applications and services we evaluated, only approximately 10% disclosed the qualitatively better response that they do not collect geolocation data about users. However, our analysis indicates that approximately 43% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 47% of applications and services evaluated discussed the qualitatively worse practice that they may collect geolocation data about users.

As discussed in the Collect PII section, this qualitatively worse finding may be the result of applications and services collecting geolocation data from children and students in order to provide the services. Although not inherently a qualitatively worse practice, the collection of generalized and precise geolocation data from children or students is not always necessary in order to use the application or service as intended.[52,53,54,55,56,57] However, the collection of geolocation information from children and students increases the risk that the information may inappropriately be used or disclosed. This finding may be the result of a lack of awareness of user concerns related to geolocation data collection. Geolocation data, far from being an isolated piece of information, may be combined with other PII to not only identify an

50 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.7.

51 General Data Protection Regulation (GDPR), Art. 5(1)(c), 7(4), 25(1).

52 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

53 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

54 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).

55 *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22577(a)(1)-(6).

56 *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(o)(1)(G).

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

individual but also to infer the individual's behavior and activities over time from their presence at a particular business or government office, and that of their friends, relatives, and associates who are near the same pinpointed location.

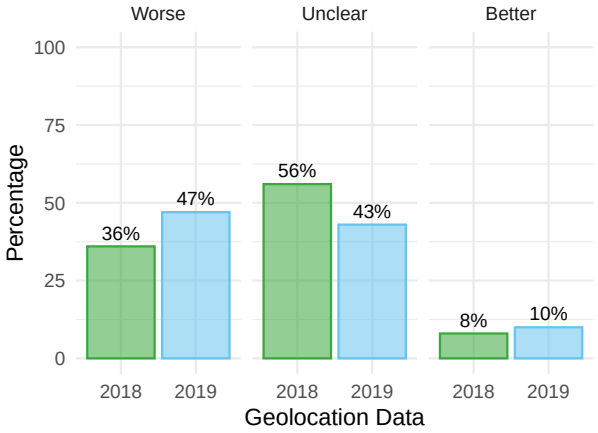


Figure 38: Do the policies clearly indicate whether or not precise geolocation data is collected?

Compared to our results in 2018, as illustrated by the above chart, applications and services evaluated in 2019 indicate an additional 2% in the qualitatively better practice of companies disclosing they do not collect geolocation data. This slightly positive trend may be the result of increased awareness that geolocation data is collected by applications and services used by children and students, and increased public concern about the collection and use of geolocation data. Applications and services need to provide greater transparency on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students but do not also disclose whether or not they collect geolocation data. As described above, geolocation data can be particularly intrusive to all users and, when combined with age data, can be especially dangerous to children and students when strangers or bad actors can locate them.

Health Data

Among the applications and services we evaluated, approximately 7% disclosed the qualitatively better response that they do not collect health and/or biometric data from users. However, our analysis indicates that approximately 82% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 11% of applications and services evaluated discussed the qualitatively worse practice that they may collect health and/or biometric data from users.

Accordingly, this finding of unclear practices may be the result of both the majority of applications and services not collecting health-related information and a fundamental misunderstanding of what constitutes health and/or biometric data as collected from children and students.[58,59,60,61,62] However, advances in facial recognition techniques, and their increasing sophistication in interpreting a variety of faces, are becoming an increased risk to children and students in particular, especially if combined with other data collected from schools and in public from cameras trained on their faces. In addition, there has been an increase in smart technology products intended for children and students that monitor their health-related information and activities during the day. Also, several states passed laws in 2018 that require schools and the state Department of Education to collect, store, and analyze increasingly sensitive information about students. For example, schools and districts have been required to collect health-related information from students as a registration requirement for the academic year.[63] Therefore, it is expected that this concern will likely see an increase in transparency year over year as companies build more smart technology products that collect health information, and also develop a better understanding of the potential implications of collecting this sensitive type of data when required by schools and districts.

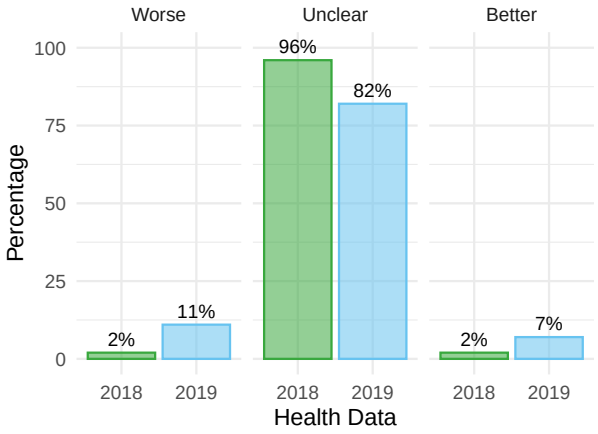


Figure 39: Do the policies clearly indicate whether or not any health or biometric data is collected?

58 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

59 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

60 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).

61 *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(b).

62 *See* General Data Protection Regulation (GDPR), Art. 4(1), 4(13), 4(14), 4(15).

63 *See* Marjory Stoneman Douglas High School Public Safety Act, 943.082, Fla. Stat. (2018).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Compared to 2018, applications and services evaluated in 2019 indicate an additional 5% in the transparent practice of companies disclosing they do not collect health and/or biometric data from users. This positive trend in usage may reflect technology advances that allow fingerprint or facial identification in lieu of a password, which apps may use as a faster means of authorized access. It is possible that many more applications and services are now using biometric technologies but fail to disclose this element of data collection in their policies. It is also possible that the increase in availability of semi-health-related apps, including those that offer meditation, reproductive health, or fitness consulting, are also collecting health data, but still, few are disclosing it with any degree of clarity.

Therefore, applications and services need to provide greater transparency and disclose better practices on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students and also fail to disclose whether they collect health and/or biometric data.

Behavioral Data

Among the applications and services we evaluated, only approximately 3% disclosed a qualitatively better response that they collect behavioral data from users. However, our analysis indicates that approximately 38% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 59% of applications and services evaluated discussed the qualitatively worse practice that they collect behavioral data from users.

As discussed in the Collect PII section, this qualitatively worse finding is likely the result of applications and services collecting behavioral information from children and students in order to provide personalized learning or assessment products. The collection of behavioral information from children or students is not always necessary in order to use the application or service as intended, and while there might be a good reason for a vendor collecting behavioral information, it is considered a worse practice because the collection and use of personal information presents more risk than not collecting behavioral information. The collection of behavioral information from children and students increases the risk that the information may inappropriately be used or disclosed. Collection of behavioral information also raises additional compliance challenges for vendors regarding the use, protection, and disclosure of that behavioral information to third parties.[64,65,66]

[64] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

[65] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

[66] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(14).

In addition, this qualitatively worse finding may be the result of strong operational financial incentives to collect data about users' behavior using the product not only for product-improvement purposes but for possible use beyond the parameters of the product. In the latter case, a product's sole purpose may appear to be educational or entertainment-related, but its primary purpose may be a data-collection device for behavioral data that can be used elsewhere and possibly in an entirely different context than that in which the data was initially gathered.

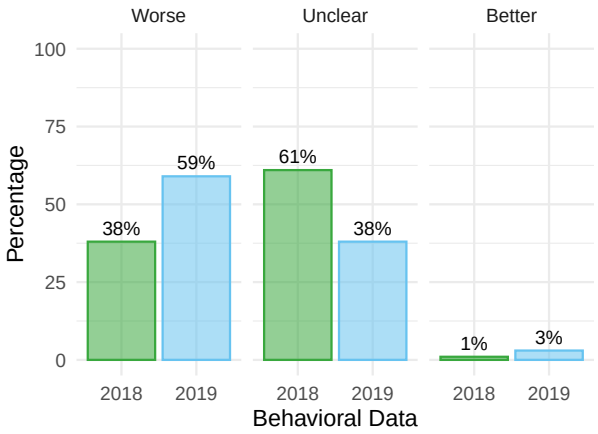


Figure 40: Do the policies clearly indicate whether or not any behavioral data is collected?

Compared to 2018, applications and services evaluated in 2019 indicate an additional 2% in the qualitatively better practice of companies not collecting behavioral data from users. This positive trend may be the result of a slight increase in understanding about the need to disclose this practice with users, but still represents a high percentage of unclear practices. In addition, there was a considerable decrease in the percentage of applications and services with unclear practices (38% in 2019 versus 61% in 2018), indicating that legal developments and educational efforts have had some positive effects on improving clarity in companies' policies on this issue.

Applications and services need to disclose better practices on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students and also fail to disclose whether they collect behavioral data. Children and students have the potential for a long digital record in front of them, and collecting (and possibly selling or storing) such behavioral information can result in privacy harms such as future difficulties in gaining admission to schools, getting job interviews, and maintaining personal relationships.

Sensitive Data

Among the applications and services we evaluated, approximately 9% disclosed the qualitatively better response that they do not collect sensitive personal information from users. However, our analysis indicates that approximately 73% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 18% of applications and services evaluated discussed the qualitatively worse practice that they collect sensitive personal information from users.

This qualitatively worse finding may be the result of some misunderstandings about the legal definition of sensitive data, how to exclude it from collection, and whether it is even necessary in order to provide the product or service. Collecting sensitive data from children and students can increase the risk of privacy harms if the information is used or disclosed in a context different from the purpose for which it was collected. The different types of sensitive information vary depending on the age of the individual and context but generally include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership and genetic data, biometric data for identification, data concerning health, or data concerning a person's sex life or sexual orientation.[67]

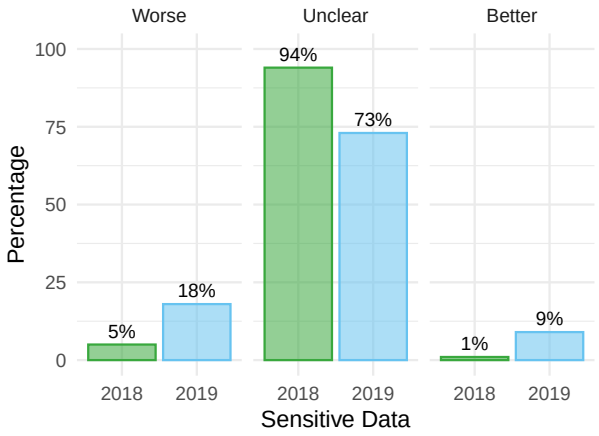


Figure 41: Do the policies clearly indicate whether or not sensitive personal information is collected?

Compared to 2018, applications and services evaluated in 2019 indicate an additional 8% in the qualitatively better practice of companies not collecting sensitive personal information from users. This positive trend is likely the result of an increased understanding and awareness that if sensitive information is collected, users should be warned about such collection and, ideally, told not to share such information or to revise their privacy settings to protect such information. More significantly, since 2018 our findings indicate a 21% decrease in the unclear practice of whether a vendor uses the product to collect sensitive personal information. We take this trend as a positive sign that if sensitive personal information is collected by an application or service that the company is making an effort to disclose this practice.

Applications and services need to disclose better practices on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services intended for children and students that do not disclose whether they collect sensitive personal information. Most users would prefer not to be required to share their sensitive personal information if it is not necessary for the operation of a product or service. Best practices should include an increased understanding that sensitive information needs to be protected if collected. If a vendor is not able or interested in incurring this additional expense, they should carefully evaluate whether or not the collection of sensitive data is absolutely necessary.

Usage Data

Among the applications and services we evaluated, approximately 92% disclosed the qualitatively worse response that they automatically collect usage information about users. However, our analysis indicates that approximately 7% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 1% of applications and services evaluated discussed the qualitatively better practice that they do not automatically collect information about users.

This significantly qualitatively worse finding is likely the result of applications and services automatically collecting usage information from children and students such as persistent identifiers, IP address, cookies, and unique device identifiers in order to facilitate remembering a user's account information and preferences when using the product. The automatic collection of usage information from children or students is invisible to the user and not always necessary in order to use the application or service as intended, and while there might be a good reason for a vendor to automatically collect usage information, it is considered a worse practice because the collection and use of more information presents more risk than not automatically collecting usage information. Some users may assume that the only data the product collects is the data the user manually enters. In that case, it is especially crucial that policies clearly articulate that data is collected automatically and, ideally, disclose the categories of data that are collected automatically, as described in the Data Categories section. The automatic collection of usage information from children and students increases the risk that the information may be inappropriately used or disclosed, as described in the Third-Party Tracking and Track

[67] *See* General Data Protection Regulation (GDPR), Processing of special categories of personal data, Art. 9(1)-(2)(a).

Users sections. Collection of usage information also raises additional compliance challenges for vendors regarding the use, protection, and disclosure of that usage information to third parties.[68,69,70,71,72,73]

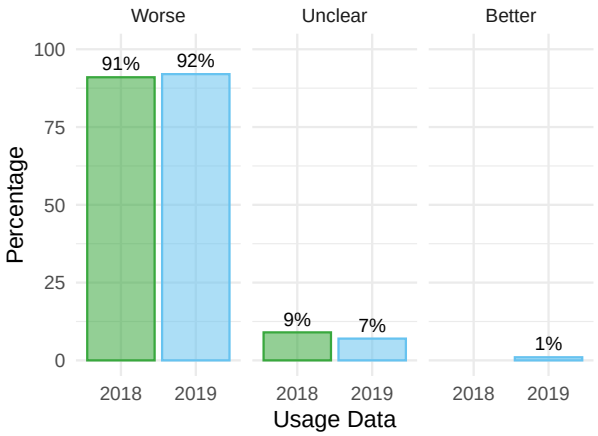


Figure 42: Do the policies clearly indicate whether or not the product **automatically** collects any information?

Compared to 2018, applications and services evaluated in 2019 indicate a marginal 1% additional result in the qualitatively better practice of companies disclosing that they do not automatically collect any information about users. We observed no indication that companies updated their policies to disclose that they do not automatically collect any information about users since 2018. Most policies, both in 2018 and 2019, indicated that they collect usage data automatically. While some of this automatic collection might be necessary for product operations, some of it may be gratuitous data collection or data collection intended for monetizing personal information, as described in the Collect PII section. Lastly, automatic data collection is an inherently nontransparent process, and users may not expect information to be collected without their explicit consent. It is difficult enough for users to keep track of the data they have voluntarily shared, and even more difficult to imagine all of the personal data that has been automatically collected.

Combination Type

Among the applications and services we evaluated, approximately 27% disclosed a qualitatively better response that they treat personally identifiable information (PII) combined with non-personally identifiable information as PII. However, our analysis indicates that approximately 70% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 3% of applications and services evaluated discussed the qualitatively worse practice that they do not treat personally identifiable information (PII) combined with non-personally identifiable information as PII.

This qualitatively worse finding is likely the result of a lack of understanding by companies of the risks of combining personally identifiable information (PII) with automatically collected non-personally identifiable information and that combined information should be treated as PII because of the additional protections required.[74] Companies typically draft privacy policies that define collected personal information from children and students and create additional rights and protections for that type of information. If personal information collected from children and students is combined with other information and is no longer treated as personal information, then children and students could lose their data rights and security protections, as described in the Data Rights and Reasonable Security sections. Some vendors may be unaware of the possibility of combining such information, in the sense that they are doing so inadvertently, or similarly inadvertently allowing others to use information that they have collected in this fashion.

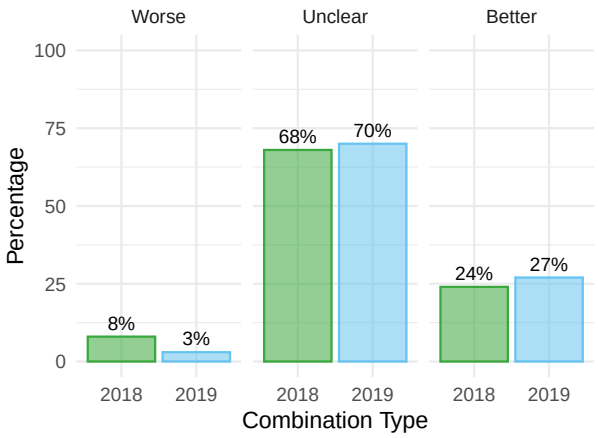


Figure 43: Do the policies clearly indicate whether or not the vendor would treat personally identifiable information (PII) combined with non-personally identifiable information as PII?

[68] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

[69] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

[70] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).

[71] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22577(a)(1)-(6).

[72] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(o)(1)(F).

[73] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(1).

[74] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

Compared to 2018, as described in the above chart, applications and services evaluated in 2019 indicate an additional 3% qualitatively better practice of treating personally identifiable information (PII) combined with non-personally identifiable information as PII. This positive trend may be the result of companies updating their policies in 2019 during a technical review of their practices and indicating that data combination was occurring, and that it should be disclosed in their policies.

Applications and services need to disclose better practices on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students but do not also disclose whether they treat personally identifiable information (PII) combined with non-personally identifiable information as PII. When these practices are not disclosed, it is difficult for users of the product to ascertain whether their private information truly remains private and if, in the course of normal business operations, such information becomes combined with non-private data.

Child Data

Among the applications and services we evaluated, approximately 21% disclosed a qualitatively better response that they do not collect personal information online from children under 13 years of age. However, our analysis indicates that approximately 15% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 64% of applications and services evaluated discussed the qualitatively worse practice that they do collect personal information from children under 13 years of age.

As discussed in the Collect PII section, this qualitatively worse finding is likely the result of applications and services collecting data from children in order to provide its products. The collection of data from children is not always necessary in order to use the application or service as intended, and while there might be a good reason for a vendor to collect personal information, it is considered a worse practice because the collection and use of personal information from children presents more risk than not collecting personal information. The collection of data from children and students increases the risk that the information may inappropriately be used or disclosed, and as a result vendors should limit the collection of data from children as discussed in the Collection Limitation section.

Accordingly, this unclear finding may be the result of inadequate age gating and verification, carelessness in ascertaining the user's age, and/or a misunderstanding of the requirements mandated by COPPA.[75] In some cases, vendors may assume that their product is not intended for children or may want to make their product less attractive to children so children will not be able to become users of their product, as described in the Intended Users section. Even when products are intended for children, it is also possible that the vendor assumes it needs personal information in order to operate the product, or collects it inadvertently when the product does not need personal information to operate and the data collection is superfluous. Moreover, because federal and state laws prohibit some of these activities involving children and students, it is possible that some of the unclear responses associated with applications and services may be because the vendors are in good faith following the law and not collecting child data, but are not clarifying this practice through their policies.[76]

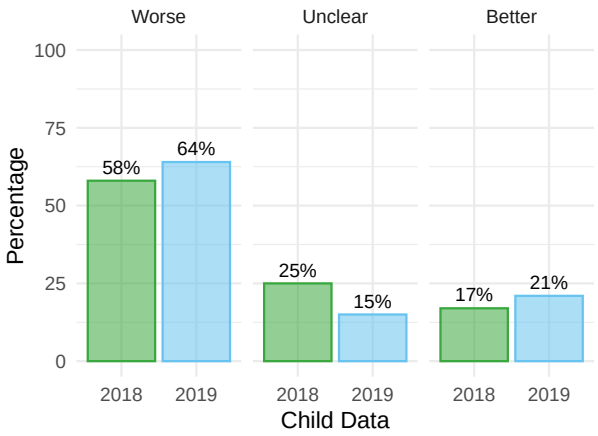


Figure 44: Do the policies clearly indicate whether or not the vendor collects personal information online from children under 13 years of age?

Compared to 2018, applications and services evaluated in 2019 indicate an additional 4% qualitatively better practice of not collecting personal information online from children under 13 years of age. This small positive trend may be the result of increased awareness of federal COPPA laws. In addition, since 2018, there has been an approximately 10% decrease in unclear practices and a 6% increase in qualitatively worse practices, which indicates that vendors updated their terms to clarify their practices related to data collection from children.

As compared to the Children Intended section, approximately 68% of applications and services disclosed they are intended for children, which indicates that at least 4% of companies have remained unclear on this issue, which may

[75] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

[76] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.4(d).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

be a violation of the requirements of COPPA if the vendor has actual knowledge they are collecting personal information from children under 13 years old. Applications and services need to disclose better practices on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students and fail to disclose whether they collect personal information from children under 13 years of age, or disclose that they do collect personal information from children under 13 years of age when it is not legally permissible to do so. Vendors need to clearly indicate their practices to protect the privacy of children and their data. When these practices are not in compliance with the law and disclosed, there is no future expectation or trust on behalf of parents, teachers, schools, or districts about how collected information from children will be handled in order to meet their expectations of privacy.

Full: Data Sharing

Evaluating data sharing takes into consideration best practices that protect the disclosure of a user's personal information to third parties.

Data Sharing Scores

Figure 45 illustrates the Data Sharing scores among all applications and services evaluated. Table 16 compares and summarizes the Data Sharing concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 16: 2018 vs. 2019 Data Sharing score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	40	69	80	75	86	95
2019	40	70	80	77	85	95

From the analysis of 10 related questions in the concern, we determined a median in 2019 of approximately 80%. This higher median is expected, given that these applications and services are intended for children and students and that a majority of companies disclose the qualitatively better practice that they limit the collection of personal information from children.

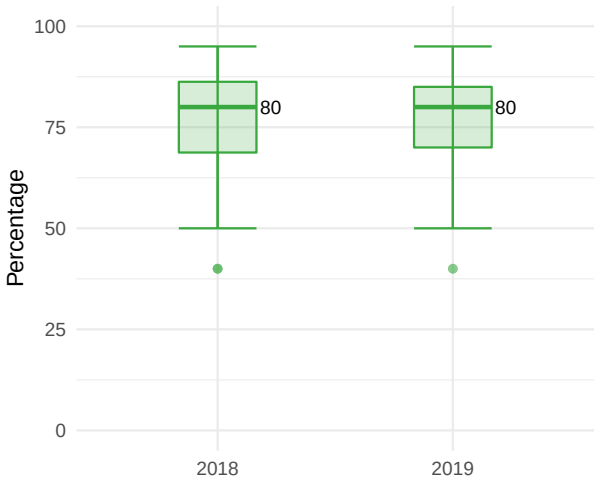


Figure 45: Comparison of Data Sharing scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of Data Collection indicate no change in median scores, which indicates that companies did not update their policies in 2019 to disclose more transparent or qualitatively better practices. Outliers that are denoted with circles in 2019 are still considered below the range of industry best practices.

Data Shared

Among the applications or services we evaluated, approximately 96% 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 and protections as the vendor's policies. This question's purpose is to provide insight into the correlation between collecting and sharing data.

As described in the Collect PII section, a similar percentage of applications and services that disclose they collect personal information also disclose that they share that information with third parties. This finding is not surprising and further supports the assumption that any application or service that collects personal information also 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 potential privacy risks and harms as well as additional compliance obligations to

protect collected data.[77,78,79,80] In addition, nontransparent responses may indicate that no personal information is collected by the application or service, or no third-party services are required to provide the service. It is important given the expectation that collected information is shared with third parties that vendors clearly share information (including data categories, uses, and names of third parties) regarding how, why, and with whom the application or service shares child or student information, as well as whether the same data rights and responsibilities outlined in the vendor's policies apply to third parties.

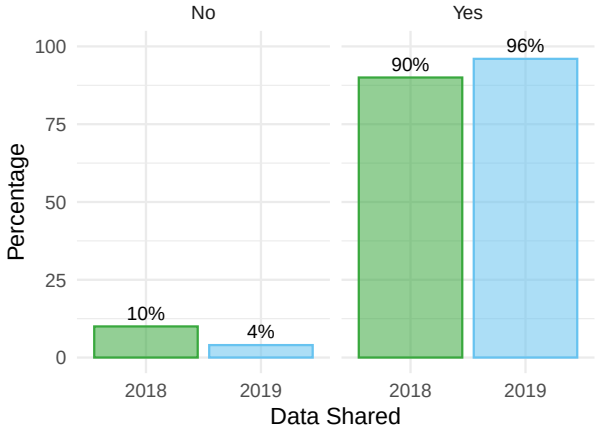


Figure 46: Do the policies clearly indicate whether collected information (this includes data collected via automated tracking or usage analytics) is shared with third parties?

Compared to 2018, applications and services evaluated in 2019 indicate a 6% increase in the sharing of collected personal and non-personal information with third parties. Respectively, there has been a decrease of approximately 6% of unclear practices. This positive trend is likely the result of companies updating their policies in 2018 to be more transparent for compliance purposes and clarifying the data-sharing practices that they may already engage in with third parties. While this disclosure of sharing data with third parties is neither qualitatively good nor qualitatively bad for our evaluation purposes, the increase in transparency practices is helpful in determining whether or not additional protections should be considered prior to using an application or service with children and students.

Data Categories

Among the applications and services we evaluated, approximately 79% disclosed the categories of information that are shared with third parties. However, our analysis indicates that approximately 21% of applications and services evaluated were nontransparent about which categories of information are shared with third parties.

Disclosing the categories of information shared with third parties provides notice to users of the application or service which personal and nonpersonal information may be processed by other companies.[81] [82] Notice of the categories of information shared is important to parents and teachers as they manage parental consent and school-compliance issues in the individual contexts in which the application or service is used. For example, different populations of students have different needs for data management, and there may be applications and services intended for children under 13 or for students with an Individualized Education Program (IEP), and therefore users need to understand which data categories are collected and shared. In addition, as discussed in the PII Categories section, approximately 92% of applications and services indicate the categories of personal information collected, and as described in the Data Shared section, approximately 96% of applications and services disclose that they share data with third parties. Therefore, applications and services need to provide greater transparency on this issue, because these products are among the 150 most popular educational technology products, and there is still a moderate percentage of applications and services that do not disclose which categories of information are shared with third parties.

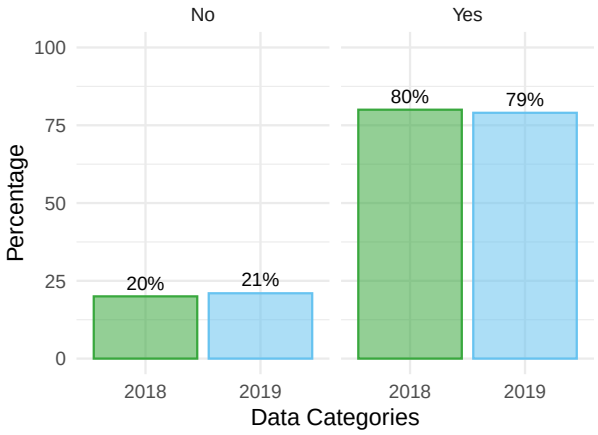


Figure 47: Do the policies clearly indicate what categories of information are shared with third parties?

77 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.8.

78 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

79 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(4), 22584(b)(4)(B)-(C),(k).

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

81 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(c)(2).

82 General Data Protection Regulation (GDPR), Art. 14(1)(d), 15(1)(b).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Compared to 2018, applications and services evaluated in 2019 indicate a marginal 1% decrease in indicating the categories of information that are shared with third parties. This plateauing trend is likely the result of companies assuming general types of information, such as personal information or usage information, are sufficient for transparency purposes. Companies with nontransparent practices should consider their compliance obligations and update their policies to disclose the specific categories of data collected by the application or service, especially when dealing with information collected and shared from children, because context is critically important when considering the privacy implications of sharing information with third parties.

Sharing Purpose

Among the applications and services we evaluated, approximately 92% disclosed the vendor's intent or purpose for sharing data with third parties. In addition, our analysis indicates that approximately 8% of applications and services evaluated were nontransparent about their intent or purpose for sharing information with third parties.

Compared to the Data Shared section, approximately 96% of applications and services disclosed the intent or purpose of sharing data with third parties, which indicates that approximately 4% need to increase their transparency on this issue. Assuming good intent, this lack of clarity is likely the result of oversight by companies in the policies. As user awareness increases and the purpose for sharing data becomes an expected response, the number of policies disclosing their sharing purpose should increase. In some cases, however, there could be a deliberate obfuscation of purpose to avoid disclosing unsafe or questionable practices. By not disclosing the reason for sharing, it is unclear whether data is used for other purposes, such as advertising, outside of the intent of the application being used.[83,84] [85,86] Disclosing the purpose of sharing data with third parties is an important part of making an informed decision of whether or not to use an application in a particular situation.

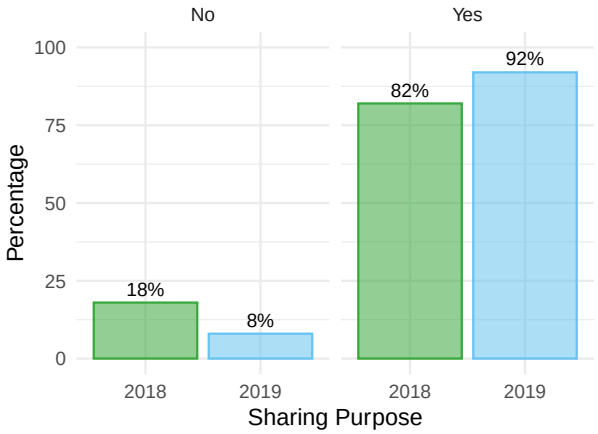


Figure 48: Do the policies clearly indicate the vendor's intention or purpose for sharing a user's personal information with third parties?

Compared to 2018, applications and services evaluated in 2019 indicate a 10% increase in companies disclosing the purpose for sharing a user's personal information with third parties. This significant positive trend is likely the result of increased legislative pressure, such as the GDPR, and consumer demand for more transparency on why their data is shared with third parties. From our analysis, it appears there is approximately a 4% lower occurrence in the disclosure of transparent practices for this issue, as compared to the Data Shared section, but a 13% higher rate of disclosure than for the Data Categories section. The transparency gap between the Data Shared and Data Categories sections has been cut in half (from 8% in 2018 to 4% in 2019) but, optimally, there should be no gap at all. The 10% increase in disclosure of sharing purpose from 2018 to 2019, combined with the 1% decrease in data categories over the same time, widened the gap from 2% to 13%. This is likely the result of the new legislative compliance obligations that require disclosures with respect to sharing data with third parties.

Lastly, this 10% increase in sharing purpose disclosures since 2018 is a significant step toward transparency with this issue, and almost all the policies that indicated data was shared with third parties were also transparent on the purpose of sharing that data. Hopefully, this trend will continue, as disclosing the purpose of sharing data is not only needed for companies to meet their compliance obligations but also to help parents and educators make informed decisions.

Purpose Limitation

Among the applications or services we evaluated, approximately 67% disclosed a qualitatively better response that the application or service limits the use of data to the educational purpose for which it was collected. However, our analysis indicates that approximately 27% of applications and

83 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

84 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(4), 22584(e)(2), 22584(b)(4)(E)(i).

85 *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(d).

86 *See* General Data Protection Regulation (GDPR), Art. 13(1)(d), 14(2)(b).

services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 6% of applications and services evaluated discussed the qualitatively worse practice that they do not limit the use of data to the educational purpose for which it was collected.

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 in the Collect PII section, where approximately 94% 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 27% 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 only the purpose for which it was collected. This difference may result in applications or services violating several federal or state laws if appropriate protections are not put in place.[87,88,89,90] In contrast, approximately 6% of applications and services disclosed qualitatively worse practices because some vendors have indicated their services are not intended for children or students, as respectively seen in the Children Intended and Students Intended sections, and therefore believe they are not required to provide limitations on their use of collected information.

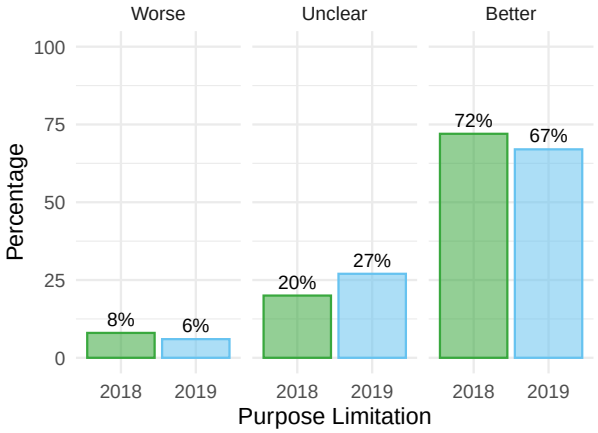


Figure 49: Do the policies clearly indicate whether or not the vendor limits the use of data collected by the product to the educational purpose for which it was collected?

Compared to 2018, applications and services evaluated in 2019 indicate a 5% decrease in the qualitatively better practice that they limit the use of data collected by the product for the purpose for which it is collected. There was also a 3% decrease in the qualitatively worse practice of disclosure of purpose limitation and approximately a 7% increase in policies that are unclear on this issue. The decrease in the qualitatively worse practices combined with the decrease in the qualitatively better practices could be explained by companies removing purpose limitation disclosures from their policies and including the practices in contractual agreements with schools and districts, as discussed in the School Contract section.

Third-Party Analytics

Among the applications and services we evaluated, approximately 4% disclosed a qualitatively better response that they do not share collected information with third parties for analytics and tracking purposes. However, our analysis indicates that approximately 17% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 79% of applications and services evaluated discussed the qualitatively worse practice that they do share collected information with third parties for analytics and tracking purposes.

Analytics is an important piece of information used to help vendors improve and troubleshoot their apps. However, using a third party to transfer and collect data can leave student data open to the possibility of data misuse and increases the risk of a data breach, as described in the Data Breach section. It is important from a user perspective to know whether their analytics data is being outsourced to a third party and what data is being shared or collected in this process. Using a third-party company for tracking purposes also puts data out of a user's control. It is important to also consider the limitation of the use of this data for product-improvement purposes. It is too easy to collect more data than is needed, and that increases the risk of exposing this information in an unintended or malicious way.

This significant qualitatively worse finding is likely the result of the ubiquity and ease of integration of analytics tools such as those provided by Google. Legislative changes in 2018 such as GDPR are increasing the need for greater transparency on this issue by forcing more transparent disclosures about a company's data analytics collection, use, automated profiling, and disclosure practices to third parties.[91,92,93]

87 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10; *See* 312.4(b).

88 California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(3).

89 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(b).

90 *See* General Data Protection Regulation (GDPR), Art. 5(1)(b), 25(2).

91 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

92 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(1)(A), 22584(b)(2).

93 *See* General Data Protection Regulation (GDPR), Processing of special categories of personal data, Art. 9(1)-(2)(j).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

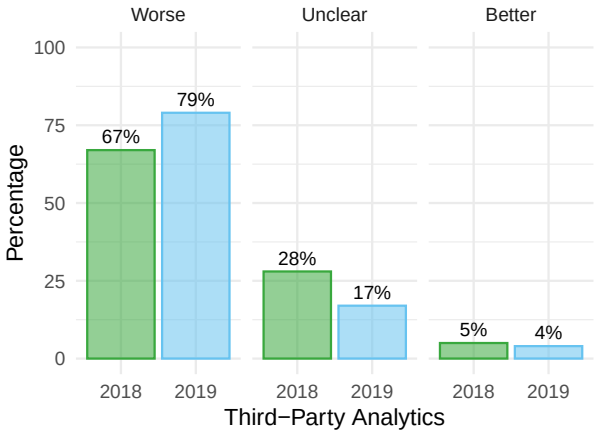


Figure 50: Do the policies clearly indicate whether or not collected information is shared with third parties for analytics and tracking purposes?

Compared to 2018, applications and services evaluated in 2019 indicate approximately no change in the qualitatively better practice that information is not shared with third parties for analytics and tracking purposes. However, since 2018, qualitatively worse practices increased approximately 12%, and unclear practices decreased respectively by 11%. This shifting from unclear to qualitatively worse practices in 2018 can likely be attributed to new privacy legislation and compliance obligations for companies combined with increased awareness and privacy expectations from users. Additionally, the ease of use and lack of financial cost of third-party analytics tools could also be a contributing factor, although the shift from unclear to qualitatively worse practices with almost no change in qualitatively better practices may indicate that companies were already engaging in these practices and simply updated their policies to be more transparent.

From our analysis, it appears that approximately 4% of applications and services are unclear with respect to whether or not data is shared with third parties, as seen in the Data Shared section, but approximately 17% are unclear with respect to Third-Party Analytics. This represents an almost 13% gap in disclosure between use of analytics and sharing data with third parties. Combining this information with the approximately 8% difference between unclear practices in Third-Party Limits would seem to indicate that third-party analytics tools are sometimes being used without considering data limitations. Lastly, applications and services need to examine the data flow when looking at their analytics tools from the standpoint of controlling and limiting data transfers to and from third-party analytics providers to only what is necessary to improve the product and provide the services without allowing extraneous data collection.

Third-Party Research Section

Among the applications and services we evaluated, approximately 6% disclosed a qualitatively better response that they do not share collected information with third parties for research or product-improvement purposes. However, our analysis indicates that approximately 43% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 51% of applications and services evaluated discussed the qualitatively worse practice that they share collected information with third parties for research or product-improvement purposes. This question is relevant to both the Data Sharing and Data Sold concern sections. To avoid repetition, further analysis of this issue is available in the Third-Party Research section in the Data Sold concern.

Third-Party Providers

Among the applications and services we evaluated, approximately 89% disclosed that third-party services are used to support the internal operations of the vendor's product. However, our analysis indicates that approximately 10% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 1% of applications and services evaluated disclosed that third-party services are not used to support the internal operations of the vendor's product.

It is imperative that vendors disclose whether they share a child or student's data with third-party service providers in order to allow parents and educators to easily determine where their data is processed and stored for compliance and accountability purposes. With increased globalization and ubiquitous availability of cloud and support services, it is sometimes difficult to determine where a child or student's personal information is actually processed and stored. Since schools are ultimately responsible for "direct control" over the first-party applications and services used by students, as described in the School Official section, they require knowledge of which third-party service providers are also handling students' personal information so appropriate contractual obligations can be put in place for additional third parties, as described in the School Contract section.

Furthermore, approximately 10% of applications and services do not disclose whether or not third-party services are used to support the internal operations of the vendor's product, which may be the result of a lack of knowledge on the part of vendors that they are required to disclose this prac-

tice for compliance purposes.[94,95,96,97,98] Privacy laws protecting children, students, and consumers are quickly changing, and companies may find it difficult to continue to update their policies every year. However, when these practices are not 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 by third-party service providers in order to meet their expectations of privacy.

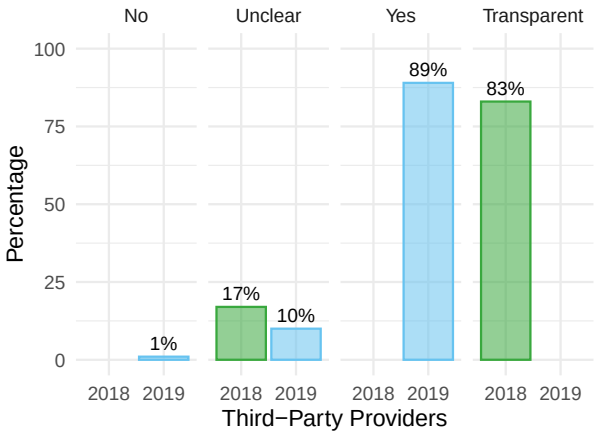


Figure 51: Do the policies clearly indicate whether or not third-party services are used to support the internal operations of the vendor's product?

Compared to 2018, applications and services evaluated in 2019 indicate a decrease of approximately 7% in unclear responses. From our analysis, it appears there is a 3% discrepancy between those vendor's indicating that third-party providers are used to support the internal operations of the vendor's product (89%) and vendors indicating the intention or purpose of sharing personal information with third parties (92%), as seen in the Sharing Purpose section. This means more companies are disclosing the purpose of sharing data with third parties, but not that the application or services actually uses third-party service providers. This surprising finding could be due to vendors indicating either they do not share information for any purpose with third parties or that third parties only help with features or functionality not related to access or processing personal information.

Third-Party Roles

Among the applications and services we evaluated, approximately 81% disclosed that they clearly indicate the role of third-party service providers. However, approximately 19% did not disclose the role of third-party service providers.

In addition to the disclosure of third parties involved in the provision of services, as described in the Third-Party Providers section, it is important to clearly explain and define the role third parties have in supporting the internal operations of the vendor's product. It is not sufficient to state that a third party is used without also clarifying how that third party uses shared information. Clarifying the role of third parties helps parents and educators make a more informed decision by better understanding the purpose of the vendor sharing data with third parties. This information is necessary to balance the risk of sharing data against the value of the additional services provided and the compliance obligations to disclose the roles of third-party providers.[99,100,101]

The percentage of applications and services with unclear policies may be the result of vendors not understanding their compliance obligation to clarify which role third parties are playing in the delivery of the product. In some cases, unclear practices may be the result of a vendor's mistaken assumption that third-party service providers are an extension of their own product and that therefore consumers do not need to know this proprietary information. In other cases, vendors may work with dozens of third-party service providers and subcontractors under nondisclosure agreements and may believe that disclosing these relationships would pose a competitive disadvantage. However, when these practices are not 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 by third-party service providers.

94 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

95 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(i).

96 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(1).

97 *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.140(d)(5), 1798.140(t)(2)(C), 1798.140(v).

98 General Data Protection Regulation (GDPR), Art. 13(1)(e), 14(1)(e), 15(1), 28(3).

99 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

100 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(i).

101 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(1).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

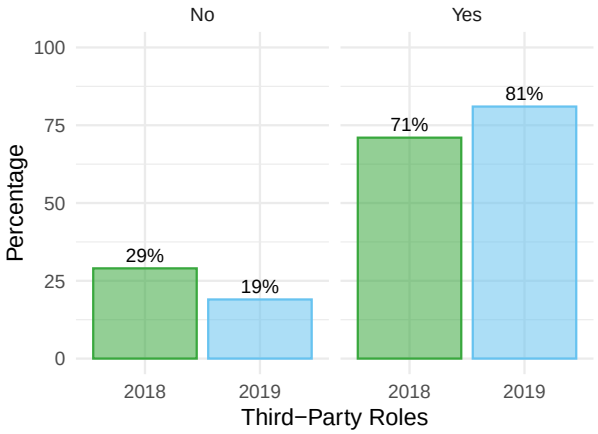


Figure 52: Do the policies clearly indicate the role of third-party service providers?

Compared to 2018, applications and services evaluated in 2019 indicate an approximate 10% increase in companies that clearly indicate the role of third-party service providers. This positive trend is likely the result of companies updating their policies in 2018 due to increased scrutiny from parents and educators with raised awareness of third-party usage, roles, and data misuse as well as additional compliance obligations. This increased scrutiny was likely the result of mainstream media headlines discussing Facebook's data misuse scandal with a third-party research and data-analysis company, Cambridge Analytica.[102]

From our analysis, it appears there is approximately a 15% lower occurrence in the disclosure of third-party service provider roles as compared to the Data Shared section. This is an improvement over the 19% we saw in 2018. However, there is still a gap between data shared with third parties and companies' disclosure of the role these third parties play in the process of supporting a given application or service. Moving forward, vendors should realize the importance of transparency on this issue and continue the positive trend of disclosing the roles of third-party service providers.

Social Login

Among the applications and services we evaluated, approximately 53% disclosed that they support social or federated login. However, our analysis indicates that approximately 43% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 4% of applications and services evaluated did not support social or federated login.

As it becomes increasingly difficult for parents and educators to manage the proliferation of applications and services that are being used by children and students on a daily basis, both at home and in the classroom, they often see social or federated login features as a quick and convenient alternative to managing countless user account names and passwords. In order to streamline the account-creation process, outsource account management, and outsource authorization practices, many vendors are incorporating new social or federated login options into their products. These additional third parties often provide this integration in exchange for their collection of Usage Data, as described in the Third-Party Providers section. While considering these third-party authorization options, it is important to understand the data collection practices of these third-party companies in addition to the data collection practices of the application or service itself. For example, third-party login services, such as an LMS or a single sign-on service like Clever, typically only provide a portal for authentication and do not collect additional student data themselves. Others, especially those with a strong social sharing context such as Facebook or Google single sign-on, harvest additional data from children or students depending on the account type as part of their own data collection purposes, as discussed in the Third-Party Tracking section. It is also important for parents and schools to consider that the data flows two ways when they're using a third-party social or federated login authorization service and that personal and usage information may be collected and used by third-party login providers in unintended ways.[103]

Accordingly, the relatively high percentage of unclear findings for social or federated login support may be due to vendors simply not offering this service, and therefore they do not believe it is necessary to disclose these practices in their policies. However, when these practices are not disclosed, there is no future expectation or trust on behalf of parents, teachers, schools, or districts concerning whether there is the use of social login.

[102] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, Mar. 15, 2017, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[103] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.6(c).

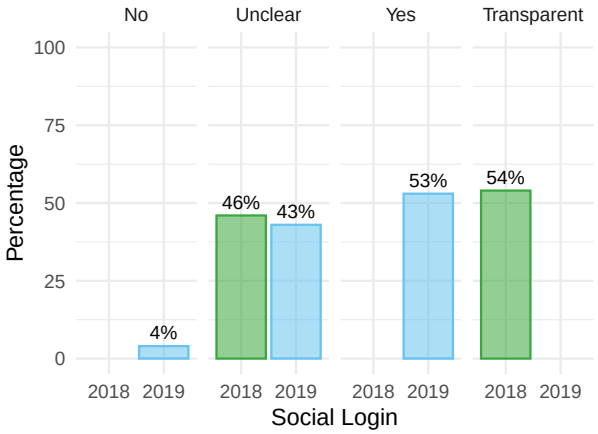


Figure 53: Do the policies clearly indicate whether or not social or federated login is supported to use the product?

Compared to 2018, applications and services evaluated in 2019 indicate a 3% increase in companies that disclose whether or not they support social or federated login. This small increase is likely the result of increased adoption of social or federated login services among edtech vendors who updated their policies to disclose new social login features. As more schools and users look for convenient consolidated managed account options, social and federated login options will be increasingly adopted by schools and districts. Therefore, it is recommended in the best interests of schools and districts that vendors clearly state in their policies whether social login is available on the application and service.

Third-Party Limits

Among the applications and services we evaluated, approximately 71% disclosed a qualitatively better response that they do impose contractual limits on how third parties can use personal information that the vendor shares or sells to them. However, our analysis indicates that approximately 25% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 4% of applications and services evaluated discussed the qualitatively worse practice that they do not impose contractual limits on how third parties can use personal information that the vendor shares or sells to them.

Without contractual limits on third-party use of data from children and students, parents and educators can no longer be assured that the privacy provisions outlined in an application or service's policies will be honored by third parties that have access to personal data. It is imperative that vendors disclose the details of their process for maintaining data integrity throughout their supply chain of third-party service providers. In some cases, a lack of disclosure may be the result of vendors otherwise meeting their compliance obligations by signing confidential contractual agreements with third-party service providers, so they therefore do not believe that consumers need to know this proprietary information.[104,105,106,107] In other cases, vendors may work with dozens of third-party service providers and subcontractors under nondisclosure agreements believed to be a competitive disadvantage if publicly disclosed in their policies. However, when these practices are not 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 protected from misuse by third-party service providers.

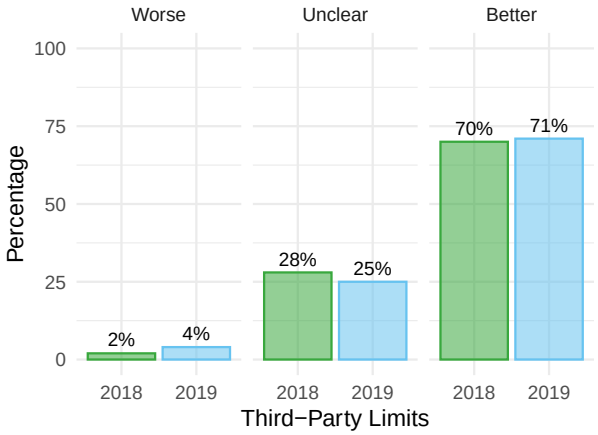


Figure 54: Do the policies clearly indicate whether or not the vendor imposes contractual limits on how third parties can use personal information that the vendor shares or sells to them?

Compared to 2018, applications and services evaluated in 2019 indicate a marginal 1% increase in the qualitatively better practice that companies do impose contractual limits on how third parties can use personal information that the vendor shares or sells to them. In addition, since 2018 there has been a 3% decrease in unclear practices and a respective 2% increase in qualitatively worse practices. From our analysis, it appears there is approximately a 25% lower occurrence in the disclosure of qualitatively better practices for this issue, as compared to the Data Shared section. This is a sizable gap between vendors disclosing that data is shared with third parties and also disclosing they impose contractual limits on third parties. Therefore, vendors should at a minimum disclose that they impose contractual limits on third-party service providers if they already engage in this practice, or con-

104 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.

105 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(B).

106 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(4)(E)(i), 2584(b)(4)(E)(ii)

107 *See* General Data Protection Regulation (GDPR), Processor, Art. 28(2)-(4), 29.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

sider changing their practices to impose contractual limits on third parties to better protect personal information gathered from children and students.

Full: Data Security

The concern of Data Security addresses practices where children 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.

Data Security Scores

Figure 55 illustrates the Data Security scores among all applications and services evaluated. Table 17 compares and summarizes the Data Security concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 17: 2018 vs. 2019 Data Security score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	0	30	40	44	60	95
2019	0	31	50	53	70	95

From the analysis of 10 related questions in the concern, we determined a median in 2019 of approximately 50%. This median is lower than expected, given that these applications and services are intended for children and students and that a majority of companies disclose the qualitatively better practice that personal information from children and students is protected with reasonable security measures.

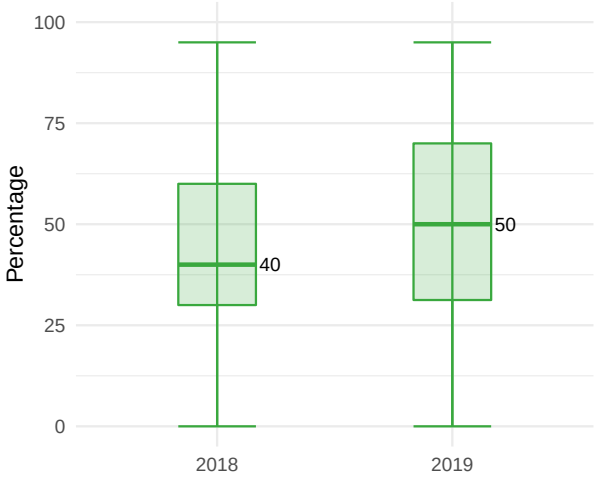


Figure 55: Comparison of Data Security scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of Data Security indicate a 25% increase in median scores that indicate more transparent and qualitatively better practices of protecting personal information with reasonable security practices.

Verify Identity

Among the applications or services we evaluated, approximately 45% disclosed the qualitatively worse response that the vendor or authorized third party verifies a user's identity with personal information. However, our analysis indicates that approximately 52% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that 3% of applications and services evaluated discussed the qualitatively better practice that they do not verify a user's identity with personal information.

This qualitatively worse finding is likely the result of applications and services collecting additional personal information from parents or educators in order to provide the services and allow authorized access to modify, export, or delete data of children and students. The collection of additional personal information from parents, educators, or children and students for verification purposes is not always necessary in order to use the application or service as intended. However, the collection of additional personal information from parents and educators, which often includes government-issued identification documents, increases the risk that the information may inappropriately be used or disclosed and is considered a worse practice from a privacy perspective. Collection of additional personal information for verification purposes also raises additional compliance challenges for vendors regarding the use, protection, and disclosure of that personal information to third parties.[108,109,110] For the purposes of this evaluation, we recommend that applications and services intended for children under 13 years of age and students not collect any additional personal information to verify users if possible, or place restrictions on the use, disclosure, and retention of sensitive data used for verification purposes, as described in the Collection Limitation section.

[108] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(2)(v); *See* 15 U.S.C. §6501(9).

[109] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(c).

[110] General Data Protection Regulation (GDPR), Art. 8(2), 12(6).

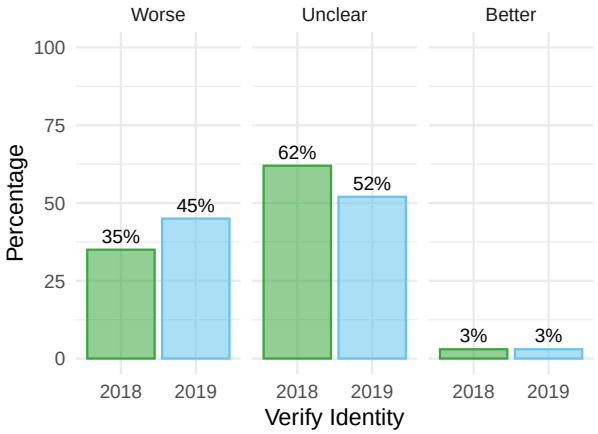


Figure 56: Do the policies clearly indicate whether or not the vendor or vendor-authorized third party verifies a user's identity with personal information?

Compared to 2018, applications and services evaluated in 2019 indicate a 10% increase in the qualitatively worse practice that the vendor or authorized third party verifies a user's identity with personal information. In addition, since 2018 there has been a respective 10% decrease in unclear practices. This shift from unclear to qualitatively worse practices may be the result of companies updating their policies to clarify their compliance obligations of obtaining verifiable information from parents and educators for parental consent purposes, and providing users the ability to export or download their data and collecting additional sensitive personal information for verification purposes. As compared to the Parental Consent section, approximately 73% indicate that they obtain verifiable parental consent before they collect or disclose personal information, but only 45% verify a parent or guardian's identity with personal information. Therefore, 28% of vendors indicate they obtain verifiable parental consent but do not also disclose that they verify a user's identity, which could result in compliance violations if the vendor or school is requested to provide verification of consent.

However, a majority of applications and services are unclear on this issue. When this type of sensitive data collection practice is not disclosed, there is no future expectation or trust on behalf of parents, teachers, schools, or districts about how collected information from parents and educators will be minimized in order to meet their expectations of privacy before using the application or service.

Account Required

Among the applications or services we evaluated, approximately 73% disclosed that the vendor requires a user to create an account to use the product. However, our analysis indicates that approximately 15% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 12% of applications and services evaluated disclosed that the vendor does not require a user to create an account to use the product.

The high number of vendors requiring an account to use the product is likely the result of applications and services providing children and students with a product that allows authorized users the ability to store their personal information and user content in a single secure location. Although not inherently a bad practice, the ability to create an account with the application service for children, students, parents, and educators is not always necessary in order to use the application or service as intended, and may prevent varying levels of risk in specific contexts. For example, an account can serve to protect a child or student's personal information and content. It can also save their strong privacy preferences, and can be managed by parents and teachers, which can enable better child and student collaboration and increase its pedagogical potential for learning. However, the collection of additional personal information from children and students to create an account increases the risk that the information may inappropriately be used or disclosed. The creation of an account requires the collection and retention of additional personal information (i.e., username, password, secret questions and answers) that could be inadvertently disclosed in a data breach to third parties, or misused by other students.

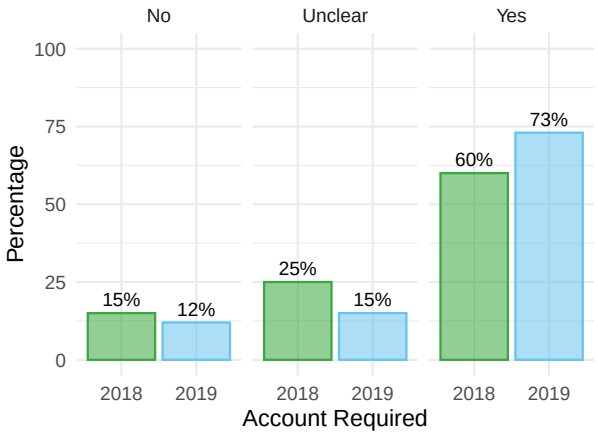


Figure 57: Do the policies indicate whether or not the vendor requires a user to create an account with a username and password in order to use the product?

Compared to 2018, applications and services evaluated in 2019 indicate a 13% increase in the practice that the vendor requires a user to create an account to use the product. In addition, since 2018 there has been a respective 10% decrease in unclear practices and a 3% decrease in vendors not requiring a user to create an account to use the product. This trend is likely the result of applications and services simply clarifying already existing account-creation processes.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Managed Account

Among the applications or services we evaluated, approximately 65% disclosed that the application or service provides user-managed accounts for a parent, teacher, school, or district. However, our analysis indicates that approximately 34% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 1% of applications and services evaluated disclosed that they do not provide user-managed accounts for a parent, teacher, school, or district.

Similarly to the Account Required section, the high number of vendors providing managed accounts is likely the result of applications and services providing children and students the ability to create an account in order to provide the services and allow authorized parents and educators to control and monitor child and student accounts with parental controls or account-creation and -assessment features. Managed accounts allow the school or district faculty to control the deployment of the application or service and administration of student account usernames and passwords, as well as to manage compliance obligations to provide parents the ability to access, review, modify, or delete their student's education records that are maintained by the educational institution.[111]

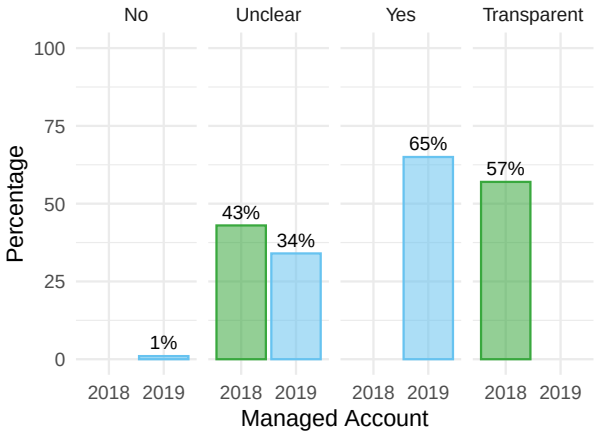


Figure 58: Do the policies clearly indicate whether or not the vendor provides user-managed accounts for a parent, teacher, school, or district?

Compared to 2018, applications and services evaluated in 2019 indicate a 9% decrease in unclear practices. This positive trend may be the result of applications and services clarifying the account-creation and -management process in their policies, which was likely a practice they already engaged in but needed to clarify in order to meet their contractual related practices of data ownership and management with schools and districts, as described in the School Contract section.

Two-Factor Protection

Among the applications or services we evaluated, approximately 25% disclosed a qualitatively better response that the application or service provides two-factor authentication (2FA). However, our analysis indicates that approximately 75% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that 0% of applications and services evaluated discussed the qualitatively worse practice that they do not provide two-factor authentication.

This qualitatively better percentage is lower than expected, but the adoption of two-factor authentication, as discussed in the Reasonable Security section, is an industry standard, and, although relatively new, its adoption 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, as discussed in the Data Breach section.

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 or have already been leaked in breached data, and passwords are easy to lose or steal, especially if they 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 account is compromised, then all of the other services they use could 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 75% of applications and services are unclear on this issue, which indicates that the industry still has a long way to go in adopting this important information-security technology.

[111] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.10, 99.20, 99.5(a)(1).

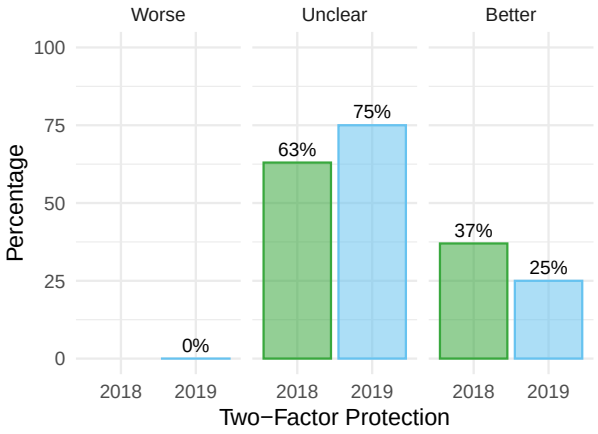


Figure 59: Do the policies clearly indicate whether or not the security of a user's account is protected by two-factor authentication?

Compared to 2018, applications and services evaluated in 2019 indicate a 12% decrease in the qualitatively better practice that companies disclose they provide two-factor authentication (2FA). This shift from qualitatively better to unclear practices is unexpected and likely the result of selection bias with the 50% additional products evaluated, or companies updating their policies to remove their disclosure of this practice but still providing the 2FA feature as part of the application or service. In addition, companies likely consider 2FA an optional self-evident feature of the application and service, rather than a differentiating advanced security practice and therefore believe they do not need to disclose that practice in their policies. However, when these types of security practices are not 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 protected with respect to 2FA.

Security Agreement

Among the applications or services we evaluated, approximately 36% disclosed a qualitatively better response that third-party service providers with access to a user's information are contractually required to provide the same level of security protections as the vendor. However, our analysis indicates that approximately 63% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 1% of applications and services evaluated discussed the qualitatively worse practice that third-party service providers with access to a user's information are not contractually required to provide the same level of security protections as the vendor.

As discussed in the Third-Party Limits section, without contractual limits on third-party use of data from children and students, parents and educators can no longer be assured that the reasonable security provisions outlined in an application or service's policies will be honored by third parties that have access to personal data.[112,113,114,115,116] In addition, security agreements with third-party service providers are considered a qualitatively better practice, because they can often mitigate complex compliance burdens on vendors to implement expensive security procedures, which ultimately better protects the data of children and students. In some cases, unclear disclosures may be the result of vendors otherwise meeting their compliance obligations by signing confidential contractual agreements with third-party service providers to enforce their security standards, so that they therefore do not believe that consumers need to know this proprietary information. In other cases, vendors may work with dozens of third-party service providers and subcontractors under nondisclosure agreements of their security practices and they may believe disclosing these policies would be a competitive disadvantage.

Compared to the Reasonable Security section, approximately 93% disclosed a qualitatively better response that reasonable security standards are used to protect the confidentiality of a child or student's personal information. Therefore, it would appear there is a 57% higher occurrence of vendors who disclose they use reasonable security standards than those that also disclose that they require third-party service providers to use the same level of security protections. However, approximately 63% of applications and services are unclear, and when security agreement practices are not 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 protected by third-party service providers.

112 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.

113 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii).

114 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(iii).

115 *See* California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).

116 *See* General Data Protection Regulation (GDPR), Art. 28(1), 32(4).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

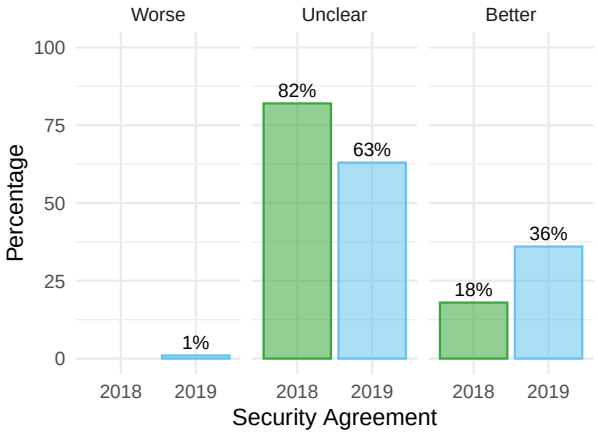


Figure 60: Do the policies clearly indicate whether or not a third party with access to a user's information is contractually required to provide the same level of security protections as the vendor?

Compared to 2018, applications and services evaluated in 2019 indicate an 18% increase in the qualitatively better practice that third-party service providers with access to a user's information are contractually required to provide the same level of security protections as the vendor. In addition, since 2018 there has been a respective 19% decrease in unclear practices. This positive trend in transparency may be the result of applications and services clarifying their security practices with third parties in response to compliance obligations to disclose third-party service providers used by the vendor and their roles, as discussed in the Third-Party Providers and Third-Party Roles sections.

Reasonable Security

Among the applications or services we evaluated, approximately 93% disclosed the qualitatively better response that reasonable security standards are used to protect the confidentiality of a child or student's personal information. However, our analysis indicates that approximately 7% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that 0% of applications and services evaluated discussed the qualitatively worse practice that they do not use reasonable security standards 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 privacy risks and harms.[117,118,119,120,121,122,123,124] 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 that collects extensive personal and behavioral information would require different reasonable security measures than 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 collected and the purpose for which it was shared, as discussed in the Collect PII, PII Categories, and Data Purpose sections. Furthermore, approximately 7% of applications and services evaluated were unclear on this issue, which may be attributable to products that collect little or no personal information and therefore do not disclose their use of reasonable security measures to protect information they do not otherwise collect. However, even services that do not collect information may be unintentionally exposing user navigation habits to unintended third parties if webpages are not served over an encrypted connection. Therefore, even applications and services that do not directly collect information may be complicit in exposing pages on their site that users may visit. For example, if a user loads a page over an unsecured connection concerning a topic like alcoholism, the information regarding which page was visited may be susceptible to interception by unintended third parties, and this information could be used in unexpected ways, such as harassment or actions that may otherwise endanger kids.

117 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(e); *See* 312.8.
118 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.
119 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii).
120 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(d)(1).
121 California Data Breach Notification Requirements, Cal. Civ. Code § 1798.81.5.
122 California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).
123 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1).
124 General Data Protection Regulation (GDPR), Art. 5(1)(f), 32(1)(b), 32(2).

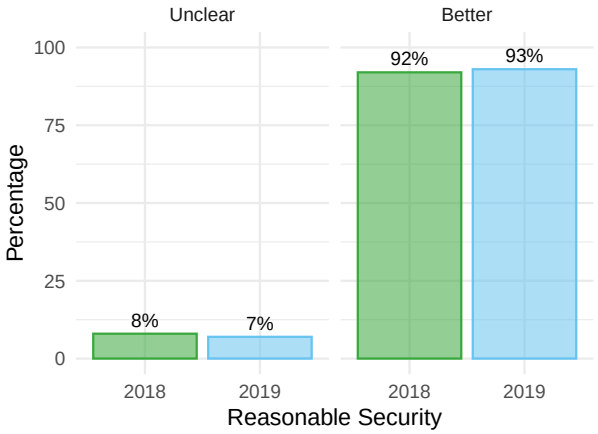


Figure 61: Do the policies clearly indicate whether or not reasonable security standards are used to protect the confidentiality of a user's personal information?

Compared to 2018, applications and services evaluated in 2019 indicate a marginal 1% increase in qualitatively better disclosures that reasonable security standards are used to protect the confidentiality of a child or student's personal information. In addition, since 2018 our findings indicate a plateau with a trivial 1% decrease in unclear practices. It is likely that companies with unclear practices assume they do not need to update their privacy policies to disclose they use reasonable security practices due to the unique nature of the application or service or limited data collection practices.

Employee Access

Among the applications or services we evaluated, approximately 51% disclosed the qualitatively better response that the vendor implements physical access controls or limits employee access to user information. However, our analysis indicates that approximately 48% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates that approximately 1% of applications and services evaluated discussed the qualitatively worse practice that the vendor does not implement physical access controls or limits employee access to user information.

Accordingly, the practice of implementing physical access controls on servers or systems that store personal information is a qualitatively better practice because it is the strongest form of security that can prevent the overriding of other software security measures. In addition, limiting employee access to personal information on a need-to-know basis also is important for protecting children and students, which includes meeting compliance obligations for training responsible individuals or employees responsible for handling personal information from children and students.[125,126] The high percentage of unclear findings is likely the result of vendors relying on third-party service providers to handle the storage of and physical access to the personal information of children and students that is located on distributed cloud-computing services or in co-location server facilities. Therefore, vendors may assume they do not need to disclose physical controls or limited employee access to personal information in their policies if they already engage in third-party contractual obligations to secure data collected from children and students, as discussed in the Third-Party Limits section. However, it should be clarified that employees either do not have access to user information or detail the additional account privileges and user roles in place to minimize employee access to only those employees that need access.

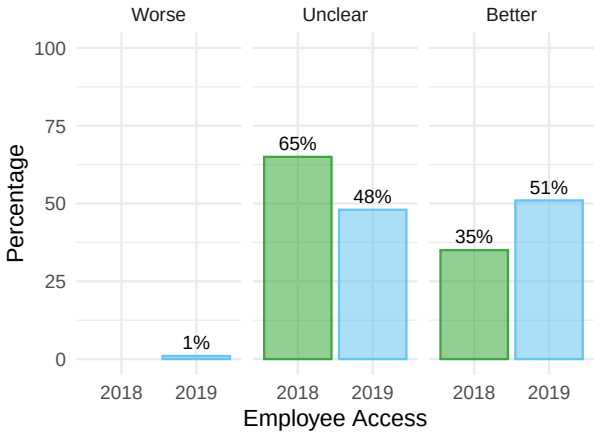


Figure 62: Do the policies clearly indicate whether or not the vendor implements physical access controls or limits employee access to user information?

Compared to 2018, applications and services evaluated in 2019 indicate a 16% increase in qualitatively better practices that the vendor implements physical access controls or limits employee access to user information. In addition, since 2018 there has been a respective 17% decrease in unclear practices. This positive trend in qualitatively better practices may be the result of applications and services clarifying their security practices with third parties in response to compliance obligations to increase their transparency with respect to third-party service providers used by the vendor and their security obligations, as discussed in the Third-Party Providers and Security Agreement sections.

[125] *See* California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).

[126] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.135(a)(3).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Transit Encryption

Among the applications or services we evaluated, approximately 52% disclosed qualitatively better practices that collected information is encrypted while in transit. However, approximately 46% of policies are unclear. In addition, approximately 2% of applications and services disclosed qualitatively worse practices that collected information is not encrypted while in transit.

This qualitatively better percentage is lower than expected, given encrypting information transmitted online is considered an industry best practice and reasonable security standard, as discussed in the Reasonable Security section. 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. This leaves some concern that services out of purview may not appropriately protect information in transit. In addition, the higher than expected percentage of unclear responses on this issue is likely attributable to a general assumption that because an application or service already discloses they provide reasonable security practices in their policies they do not need to also disclose the particular details of those 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 also require notice of compliance.[127,128,129]

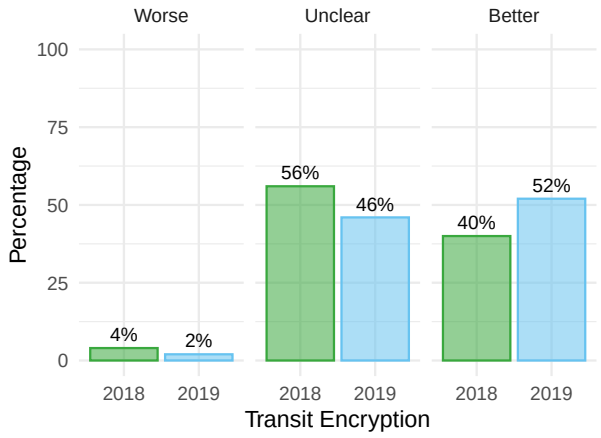


Figure 63: Do the policies clearly indicate whether or not all data in transit is encrypted?

Compared to 2018, applications and services evaluated in 2019 indicate a 12% increase in qualitatively better disclosures that collected information is encrypted while in transit. In addition, since 2018 there has been a respective decrease of approximately 10% in unclear practices. This trend may be the result of companies in 2019 updating unclear policies with better practices of using encryption of information while in transit, which is a practice they likely already engaged in.

Storage Encryption

Among the applications or services we evaluated, approximately 39% disclosed qualitatively better practices that collected information is encrypted while in storage. However, our analysis indicates approximately 58% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 3% of applications and services evaluated discussed qualitatively worse practices that information is not encrypted while in storage.

Similarly to the Transit Encryption section, this qualitatively better 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. Our evaluation process limits its analysis to only 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 in an encrypted or unreadable format.

This unclear finding is higher than expected given 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 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.[130,131] As compared to the Transit Encryption section, an additional 12% of applications and services were unclear in their policies about whether they actually encrypt collected information while in storage. Because 93% disclose reasonable security practices are used in the Reasonable Security section, a majority of unclear re-

127 Common Sense Media, *Our 2019 EdTech Security Survey*, Privacy Program (March 2019), https://www.commonsense.org/education/articles/our-2019-edtech-security-survey.

128 *See* California Data Breach Notification Requirements, Cal. Civ. Code § 1798.81.5.

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

130 *See* California Data Breach Notification Requirements, Cal. Civ. Code § 1798.81.5.

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

sponses should disclose if they engage in the qualitatively better practice of encrypting stored information.

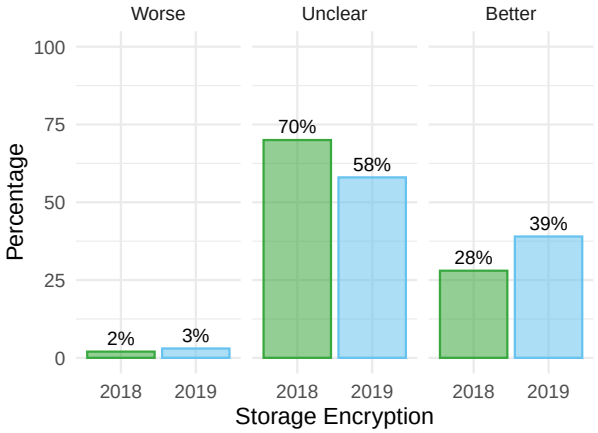


Figure 64: Do the policies clearly indicate whether or not all data at rest is encrypted?

Compared to 2018, applications and services evaluated in 2019 indicate an 11% increase in qualitatively better disclosures that collected information is encrypted while in storage. In addition, since 2018 there has been a respective decrease of approximately 12% in unclear practices. This trend may be the result of companies in 2019 updating their policies with practices they already engaged in.

Breach Notice

Among the applications or services we evaluated, approximately 50% disclosed qualitatively better practices that in the event of a data breach, if unencrypted collected information is disclosed to unauthorized individuals, the vendor will provide notice to any users affected. However, our analysis indicates approximately 47% of applications and services evaluated are unclear on this issue. In addition, approximately 3% of applications or services evaluated indicate they do not provide notification to users in the event of a data breach.

Accordingly, providing notice to users that their unencrypted information has been disclosed to unauthorized individuals is considered a qualitatively better practice and also required by various U.S. State laws.[132,133,134,135] This qualitatively worse finding may be attributable to vendors disclosing they are not responsible for providing data breach notifications to users in the event their collected information is disclosed to unauthorized individuals because any breach notice would have to originate with their third-party service provider, and not themselves. However, it is recommended that applications and services explain their data breach notification policy and any contractual obligations of third-party service providers, as described in the Third-Party Providers section, who may be providing notification to users on behalf of the company to ensure parents, teachers, schools, and districts are adequately notified.

Moreover, applications and services with unclear practices on this issue are unexpected given a majority of U.S. States have data breach notification compliance obligations that vendors are required to follow.[136] Vendors may 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 timeframe. 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 a company's data breach process will allow affected users to more quickly and adequately respond by increasing vigilance or availing themselves of additional protections such as a credit freezes or identify-theft notification services in the event of a data breach.

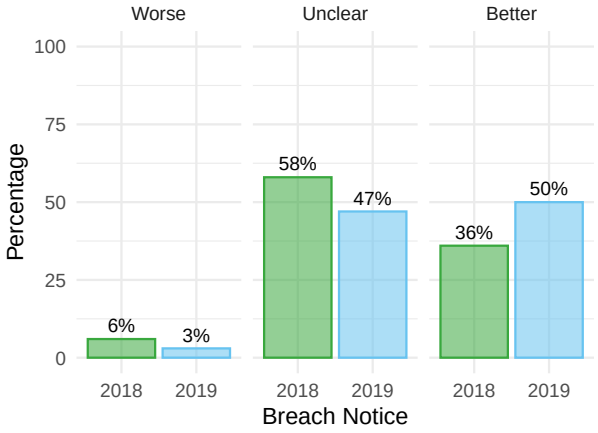


Figure 65: Do the policies clearly indicate whether or not the vendor provides notice in the event of a data breach to affected individuals?

Compared to 2018, applications and services evaluated in 2019 indicate a 14% increase in qualitatively better disclosures that the vendor will provide notice to any users af-

132 California Data Breach Notification Requirements, Cal. Civ. Code §§ 1798.29, 1798.29(h)(4), 1798.82.

133 California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(6).

134 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1)(A)-(C).

135 General Data Protection Regulation (GDPR), Definitions, Art. 4(12), 33(1)-(5), 34(1)-(3).

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

fected in the event of a data breach. In addition, since 2018 there has been a respective decrease of approximately 11% in unclear practices. This positive trend is likely the result of companies updating their policies with better practices of providing notice to any users affected in the event of a data breach, in response to greater consumer awareness of this issue given the increased number of media headlines in 2018 disclosing major data breaches involving the personal information of hundreds of millions of users.

Full: Data Rights

The concern of Data Rights addresses the practices of collecting personal information and user generated content and allowing users to exercise their rights to access, review, modify, delete, and export their personal information.

Data Rights Scores

Figure 66 illustrates the Data Rights scores among all applications and services evaluated. Table 18 compares and summarizes the Data Rights concern score minimum, maximum, median, mean, Q1 (point between the 1st and 2nd quartile), and Q3 (point between the 3rd and 4th quartile).

Table 18: 2018 vs. 2019 Data Rights score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	10	40	60	55	75	95
2019	10	60	75	69	85	95

From the analysis of 10 related questions in the concern, we determined a median in 2019 of approximately 75%. This median is lower than expected, given these applications and services are intended for children and students and a majority of companies disclose qualitatively better practices that they allow users to exercise their rights to access, review, modify, delete, and export their personal information. However, one particular question regarding User Submission or creation of content in this concern had a relatively high percentage of qualitatively worse practices because the collection of user generated content contains personal and sensitive information that could include audio, photographs, and video content of a child or student.

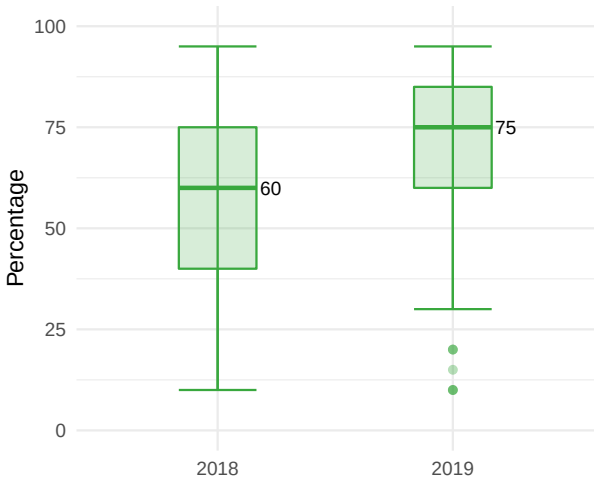


Figure 66: Comparison of Data Rights scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of Data Rights indicate a 25% increase in median scores that indicate more transparent and qualitatively better practices of allowing users to exercise their rights to access, review, modify, delete, and export their personal information. In addition, since 2018, the industry has consolidated its range of scores and significantly improved its practices regarding Data Rights as seen by the 2019 median of approximately 75% equalling the upper quartile of the 2018 range of scores for the concern of Data Rights. Lastly, because the industry has significantly improved its Data Rights practices since 2018, outliers that are denoted with circles in 2019 are now considered below the range of industry best practices and should update their terms to allow users to exercise their privacy rights.

Collection Consent

Among the applications and services we evaluated, approximately 63% disclosed a qualitatively better response that the company requests opt-in consent from a user at the time information is collected. However, our analysis indicates approximately 33% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 4% of applications and services evaluated discussed qualitatively worse practices that they do not require opt-in consent from a user at the time information is collected.

This unclear finding may be the result of companies assuming that consent is obtained from users at the point of registration for an account with an application or service when they agree to the company's terms of use and privacy policies. However, because both Federal and State law clearly prohibit collecting personal information without consent, it is possible that a large majority of unclear applications and services are in good faith following the law and collecting

consent upon registration or use of the application or service, but simply failing to disclose this practice in their policies.

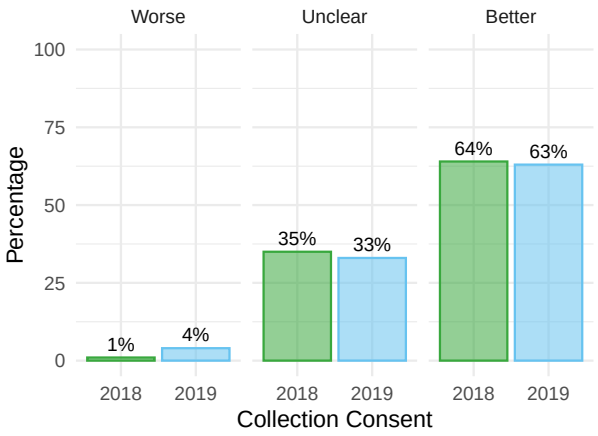


Figure 67: Do the policies clearly indicate whether or not the vendor requests opt-in consent from a user at the time information is collected?

Compared to 2018, applications and services evaluated in 2019 indicate a negligible 1% decrease in qualitatively better practices that companies request opt-in consent from a user at the time information is collected. However, since 2018, approximately 3% of applications and services have changed their unclear practices and disclosed qualitatively worse practices that they do not request opt-in consent from a user at the time information is collected. This negative trend may be the result of companies shifting their compliance obligations of providing data rights to users onto the schools or districts. For example, if a school or district has entered into a contract with a company to provide them an application or service to its students, the company typically transfers the obligation and liability under COPPA and FERPA to obtain consent for the collection, use, and disclosure of personal information to the school or district.[137,138,139] In addition, as discussed in the School Consent section these agreements typically require a school or district representative to obtain consent and respond to requests directly from parents and teachers on behalf of students to access, modify, or delete student education records. Therefore, this qualitatively worse trend could increase year-over-year as companies shift their data rights compliance costs onto schools and districts. Companies with unclear practices may seek to update their policies to shift these legal obligations in order to avoid having to also respond directly to data rights requests from parents and teachers.

User Control

Among the applications and services we evaluated, approximately 69% disclosed a qualitatively better response that a user can control the company's or third party's use of their information through privacy settings. However, our analysis indicates approximately 30% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 1% of applications and services evaluated discussed qualitatively worse practices that a user cannot control the company's or third party's use of their information through privacy settings.

This unclear finding may be the result of companies assuming that privacy settings or user controls for their personal information are features of the product and not practices that would need to be disclosed in their policies. In addition, companies may believe that because they provide privacy settings for users within the application or service, these features are obvious and therefore do not need discussion in their policies. However, providing information about a product's privacy settings and controls that users have with their personal information needs to be disclosed to users in a company's policies before they provide their data to an application or service, not afterward.

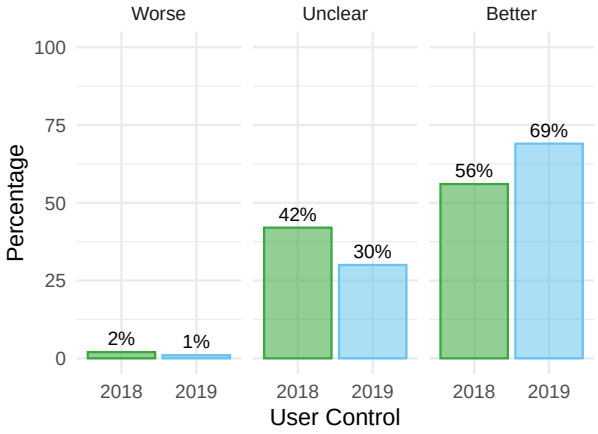


Figure 68: Do the policies clearly indicate whether or not a user can control the vendor or third party's use of their information through privacy settings?

Compared to 2018, applications and services evaluated in 2019 indicate a 13% increase in qualitatively better practices that companies disclose a user can control the company's or third party's use of their information through privacy settings. In addition, since 2018, there has been a respective 12% decrease in unclear practices. This positive trend is likely the result of companies updating their policies for compli-

137 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d).

138 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

139 *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(11), 6(1)(a), 7(1)-(2).

ance purposes to incorporate new privacy rights granted by changing International and U.S. state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018, and provided many new privacy rights for companies subject to the GDPR's requirements with the ability for users to control these new privacy settings.

User Submission

Among the applications and services we evaluated, approximately 79% disclosed a qualitatively worse response that users can create or upload content to the product. However, our analysis indicates approximately 20% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates only approximately 1% of applications and services evaluated discussed qualitatively better practices that users can create or upload content to the product.

Accordingly, allowing children and students to create or upload content to an application or service is considered qualitatively worse in our evaluation process, because user-generated content often contains personal or sensitive information in text, audio, photographs, or videos that if inadvertently disclosed that could cause serious privacy risks and harms.[140] This qualitatively worse finding is the result of many applications and services providing robust collaboration and content creation and sharing features for children and students.

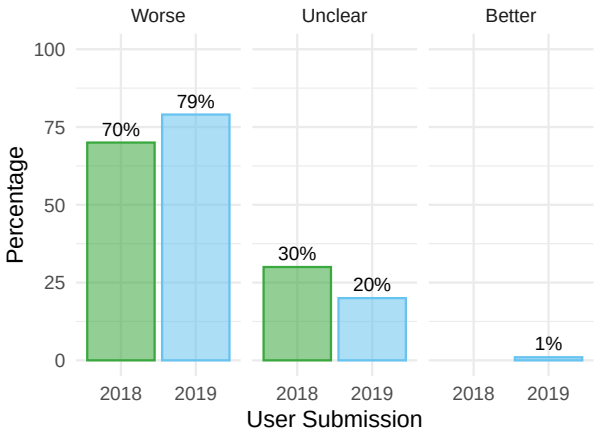


Figure 69: Do the policies clearly indicate whether or not a user can create or upload content to the product?

Compared to 2018, applications and services evaluated in 2019 indicate a 9% increase in qualitatively worse practices that companies disclose users can create or upload content to the product. In addition, since 2018 there was approximately a 10% respective decrease in unclear practices to become more transparent. This negative trend may be the result of companies adding new features that allow users to create and upload content to the application and service. However, given that the collection of any personal or sensitive personal information is a privacy risk, there are other privacy practices that companies can disclose in their policies to mitigate this risk by providing privacy settings for users to Control Visibility of their content and who they share it with, in addition to using reasonable security practices as discussed in the Reasonable Security section, to protect content from inadvertent disclosure in a data breach.

Data Ownership

Among the applications and services we evaluated, approximately 61% disclosed a qualitatively better response that a student, educator, parent, or the school retains ownership to the Intellectual Property rights of the data collected or uploaded to the product. However, our analysis indicates approximately 34% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 5% of applications and services evaluated discussed qualitatively worse practices that a student, educator, parent, or the school does not retain ownership to the Intellectual Property rights of the data collected or uploaded to the product.

This unclear finding is the result of companies not disclosing a copyright license provision in their privacy policy or terms of use for user-generated content provided by users of the application or service.[141,142] This finding is consistent with our analysis in the User Submission section that approximately 20% of applications and services are unclear about whether users can create or upload content; ostensibly because those features are not available with their application or service. However, it appears that even for companies that do disclose a copyright license provision in their policies for the right to reproduce and display a user's personal information and content, they do not explicitly state that a user retains their authorship rights in their generated content because it is implied in the requirement that the company seek a copyright license from the user for their content.

[140] Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). Privacy risks and harms, San Francisco, CA: Common Sense Media.

[141] California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(1)

[142] *See* Copyright Act of 1976, 17 U.S.C. § 102.

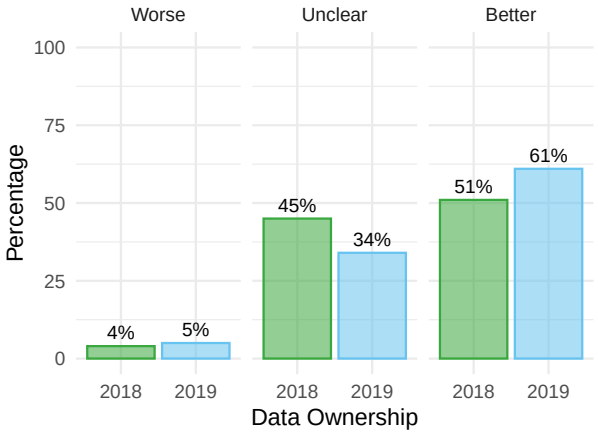


Figure 70: Do the policies clearly indicate whether or not a student, educator, parent, or the school retains ownership to the Intellectual Property rights of the data collected or uploaded to the product?

Compared to 2018, applications and services evaluated in 2019 indicate a 10% increase in qualitatively better practices that companies disclose that a student, educator, parent, or the school retains ownership to the Intellectual Property rights of the data collected or uploaded to the product. This increase is the result of a respective 11% decrease in unclear practices. This positive trend may be the result of a corresponding increase of 8% in our analysis in the User Submission section that more applications and services provide features for users to create and upload content, and therefore have also updated their policies to reflect more transparency of the intellectual property rights of the company and users with respect to the authorship of their content.

Access Data

Among the applications and services we evaluated, approximately 85% disclosed a qualitatively better response that they provide users a method to access their personal information. However, our analysis indicates approximately 14% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 1% of applications and services evaluated discussed qualitatively worse practices that they do not provide users a method to access their personal information.

This unclear finding may be associated with the practice of companies who enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent requests to access and review that data from eligible students, teachers, and parents. These companies may assume that because the contract discloses the school or district faculty control the deployment of the application or service and administration of student accounts they do not also need to disclose that practice in their policies. In addition, if the school or district enters into a contract with an edtech provider to provide services to its students, these agreements typically require a school or district representative to respond to requests directly from parents and teachers on behalf of students to access, modify, or delete student education records.

However, if there is no contract in place between the edtech provider and school or district, but the product is used in classrooms by students, then the parent on behalf of their minor child under COPPA, or teacher under FERPA can contact the edtech provider and request access to review the respective child's or student's educational record.[143,144,145,146] The edtech vendor is obligated under federal and state law and any obligations promised in their policies. Therefore, as discussed in our analysis in the School Consent section, these edtech vendors likely specify in their policies that they transfer legal obligations under COPPA and FERPA to obtain consent and provide data access requests to the schools and districts to avoid having to respond directly to parents and teachers. However, practically speaking, companies may already respond directly to parents that the product already provides logged-in account options to access and review student information records because it is simply not cost effective for a company to respond to tens of thousands of parent or teacher requests to manually provide access to student information records.

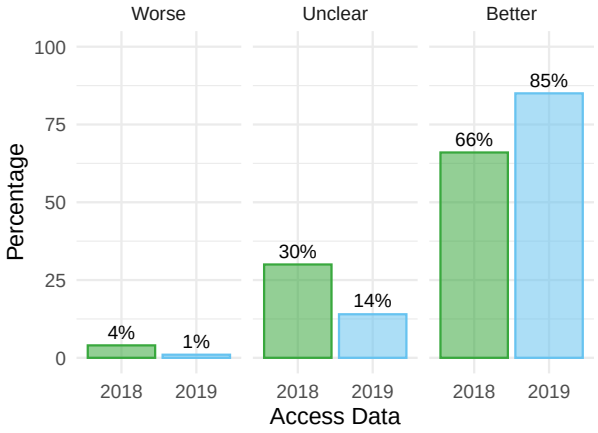


Figure 71: Do the policies clearly indicate whether or not the vendor provides authorized individuals a method to access a user's personal information?

143 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.3(c), 312.4(d)(3), 312.6.

144 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.10, 99.20.

145 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(2).

146 *See* General Data Protection Regulation (GDPR), Art. 13(2)(b), 14(2)(c), 15(1).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Compared to 2018, applications and services evaluated in 2019 indicate a significant 19% increase in qualitatively better practices that companies disclose that they provide users a method to access their personal information. In addition, since 2018 there has been a respective decrease of approximately 16% of unclear practices. Similarly to our analysis in the User Control section, this positive trend is likely the result of companies updating their policies for compliance purposes to incorporate new privacy rights granted by changing International and U.S., state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018 and provided many new privacy rights for companies subject to the GDPR's requirements with the ability for users to access and review their personal information.

Data Modification

Among the applications and services we evaluated, approximately 80% disclosed a qualitatively better response that they provide users with the ability to modify their inaccurate data. However, our analysis indicates approximately 19% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 1% of applications and services evaluated discussed qualitatively worse practices that they do not provide users with the ability to modify their inaccurate data.

As discussed in the Access Data section, this unclear finding may be associated with the practice of companies that enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent requests to access and modify that data from eligible students, teachers, and parents. These companies may assume that because the contract discloses the school or district faculty control the deployment of the application or service and administration of student accounts they do not also need to disclose that practice in their policies. In addition, if the school or district enters into a contract with an edtech provider to provide services to its students, these agreements typically require a school or district representative to respond to requests directly from parents and teachers on behalf of students to access, modify, or delete student education records.[147,148,149] However, when data modification 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.

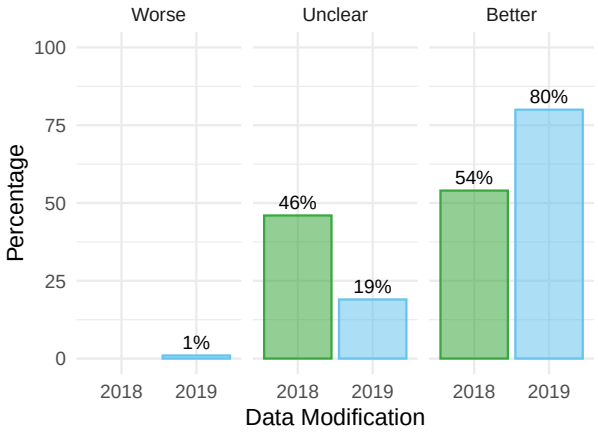


Figure 72: Do the policies clearly indicate whether or not the vendor provides authorized individuals with the ability to modify a user's inaccurate data?

Compared to 2018, applications and services evaluated in 2019 indicate a significant 26% increase in qualitatively better practices that companies disclose that they provide users a method to access their personal information. In addition, since 2018, there has been a respective significant decrease of approximately 27% of unclear practices. Similarly to our analysis in the Access Data section, a relatively similar percentage of applications and services disclose qualitatively better practices that they provide users with data rights to access, modify, or delete their personal information. Moreover, similar to our analysis in the User Control section, this positive trend is likely the result of companies updating their policies for compliance purposes to incorporate new privacy rights granted by changing International and U.S. state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018, and provided many new privacy rights for companies subject to the GDPR's requirements with the ability for users to access, review, and modify their personal information.

Retention Policy

Among the applications and services we evaluated, approximately 77% disclosed a transparent response that they have a 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 product. However, our analysis indicates approximately 23% of applications and services evaluated are nontransparent on this issue.

As discussed in the Access Data section, this nontransparent finding may be the result of companies that enter into contracts with schools and districts and require the school or district to create their own retention policy of collected personal information. These companies may assume that because the contract discloses the school or district faculty

147 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10, 99.20.

148 *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(2).

149 *See* General Data Protection Regulation (GDPR), Art. 16.

control the deployment of the application or service and administration of student accounts they do not also need to disclose in their policies that the school or district determines any retention and deletion policy.[150,151,152] However, when retention 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.

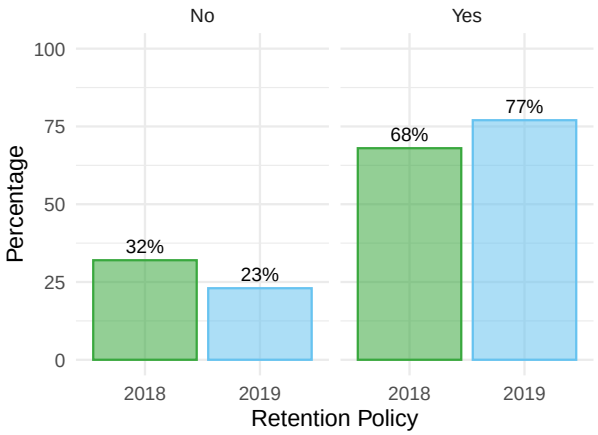


Figure 73: Do the policies clearly indicate the vendor's data retention policy, including any data sunsets or any time period after which a user's data will be automatically deleted if they are inactive on the product?

Compared to 2018, applications and services evaluated in 2019 indicate a 9% increase in transparent practices that companies disclose they have a 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 product. In addition, since 2018 there is a respective 9% decrease in nontransparent practices. This positive trend may be the result of companies updating their policies to be more transparent about already existing data retention practices given they are also updating their policies to disclose more data rights for users and to disclose how they use personal information that is collected. It is likely that companies responded to greater consumer awareness of this issue given the increased number of media headlines in 2018 disclosing major data breaches involving the personal information of hundreds of millions of users. Lastly, companies may have increased their transparency on this issue for compliance purposes when purchasing data breach insurance in 2018 which required they delete personal information when retained beyond its primary purpose to provide the application or service, or when parental consent is withdrawn in order to mitigate potential liability in the event of a data breach.

User Deletion

Among the applications and services we evaluated, approximately 66% disclosed a qualitatively better response that users can delete all of their personal and non-personal information from the vendor. However, our analysis indicates approximately 24% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 10% of applications and services evaluated discussed qualitatively worse practices.

As discussed in the Access Data section, this unclear finding may be the result of companies that enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent requests to delete that data from eligible students, teachers, and parents. These companies may be assuming that because the contract discloses the school or district faculty control the deployment of the application or service and administration of student accounts they do not also need to disclose that practice in their policies.[153,154,155] In addition, if the school or district enters into a contract with an edtech provider to provide services to its students, these agreements typically require a school or district representative to respond to requests directly from parents and teachers on behalf of students to access, modify, or delete student education records. However, when user deletion 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.

150 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10.

151 *See* California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(7).

152 General Data Protection Regulation (GDPR), Art. 13(2)(a), 14(2)(a), 15(1)(d).

153 *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(2).

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

155 *See* General Data Protection Regulation (GDPR), Right to erasure, Art. 17(2).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

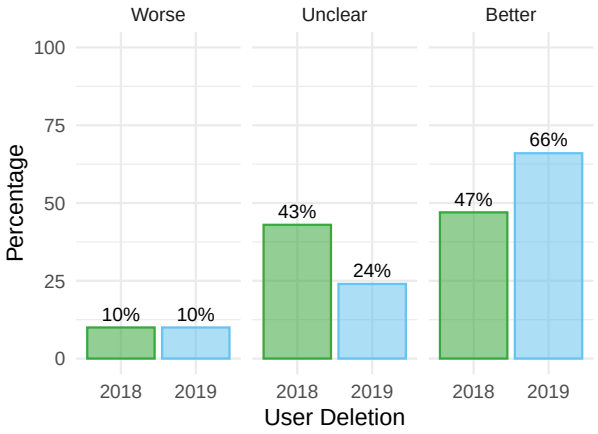


Figure 74: Do the policies clearly indicate whether or not a user can delete all of their personal and non-personal information from the vendor?

Compared to 2018, applications and services evaluated in 2019 indicate a 19% increase in qualitatively better practices that companies disclose users can delete all of their personal and non-personal information from the vendor. In addition, since 2018 there has been a respective significant decrease of approximately 19% of unclear practices. Similarly to our analysis in the Access Data section, a relatively similar percentage of applications and services disclose qualitatively better practices that they provide users with data rights to access, modify, or delete their personal information. Moreover, similar to our analysis in the User Control section, this positive trend is likely the result of companies updating their policies for compliance purposes to incorporate new privacy rights granted by changing International and U.S. state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018, and provided many new privacy rights for companies subject to the GDPR's requirements with the ability for users to access, modify, and delete their personal information.

Deletion Process

Among the applications and services we evaluated, approximately 76% disclosed a qualitatively better response that they provide a process for the school, parent, or eligible student to delete a student's personal information. However, our analysis indicates approximately 24% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates zero percent of applications and services evaluated discussed qualitatively worse practices.

As discussed in the Access Data section, this unclear finding may be the result of companies that enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent requests to delete that data from eligible students, teachers, and parents.[156,157,158,159,160,161] These companies likely assume that because the contract discloses the school or district faculty control the deployment of the application or service and administration of student accounts they do not also need to disclose that practice in their policies. In addition, if the school or district enters into a contract with an edtech provider to provide services to its students, these agreements typically require a school or district representative to respond to requests directly from parents and teachers on behalf of students to access, modify, or delete student education records.

From our analysis in the User Deletion section, it appears there is approximately a 10% lower occurrence in the disclosure of qualitatively worse practices for this issue, with a respective 10% increase in qualitatively better practices that there is a process for the school, parent, or eligible student to delete a student's personal information. This trend may be because companies that disclose users cannot delete any of their personal information from the company are transferring those compliance obligations on to the school or district to respond to requests directly from parents and teachers on behalf of students to delete student education records. However, when deletion process 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.

156 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(c), 312.4(d)(3), 312.6.

157 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.10, 99.20, 99.5(a)(1).

158 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(d)(2).

159 *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.6(c).

160 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.105(a)-(c).

161 *See* General Data Protection Regulation (GDPR), Art. 13(2)(b), 14(2)(c), 15(1)(e), 17(1)(b), 19.

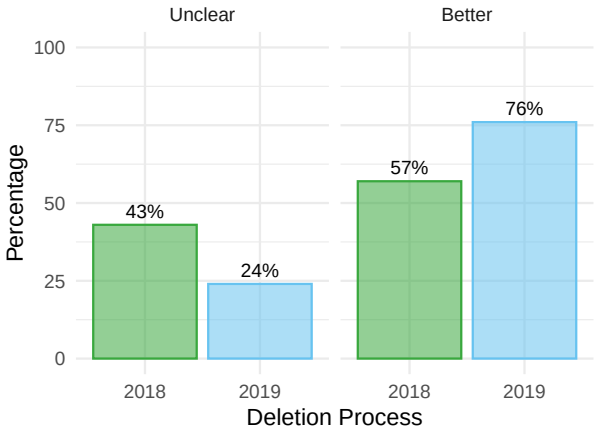


Figure 75: Do the policies clearly indicate whether or not the vendor provides a process for the school, parent, or eligible student to delete a student's personal information?

Compared to 2018, applications and services evaluated in 2019 indicate a 19% increase in qualitatively better practices that companies disclose they provide a process for the school, parent, or eligible student to delete a student's personal information. In addition, since 2018, there has been a respective significant decrease of approximately 19% of unclear practices. Similarly to our analysis in the Access Data section, a relatively similar percentage of applications and services disclose qualitatively better practices that they provide users with data rights to access, modify, or delete their personal information. Moreover, similar to our analysis in the User Control section, this positive trend is likely the result of companies updating their policies for compliance purposes to incorporate new privacy rights granted by changing International and U.S., state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018, and provided many new privacy rights for companies subject to the GDPR's requirements with the ability for users to access, modify, and delete their personal information.

User Export

Among the applications and services we evaluated, approximately 40% disclosed a qualitatively better response that a user can export or download their data, including any user-created content on the product. However, our analysis indicates approximately 57% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 3% of applications and services evaluated discussed qualitatively worse practices that they a user cannot export or download their data, including any user-created content on the product.

This unclear finding may be the result of companies unaware of their compliance obligations to provide users their information in an electronically useable format. However, U.S. state laws and the GDPR provide a right to data portability in certain circumstances, which allows a user to receive, and transmit to another vendor, their personal data in a commonly used, machine-readable format.[162,163,164] In addition, the CCPA provides a similar right for a consumer to have their information provided electronically in a readily useable format that allows the consumer to easily transmit the information to another entity.[165] From our analysis in the Access Data, Data Modification, and Data Deletion sections, it appears there is approximately a 30% higher occurrence in the disclosure of qualitatively better practices of data rights for users to access, modify, and delete their data, as compared to disclosing the data right of exporting a user's information from the application or service. However, when data export 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 available to take with them to other applications and services in order to meet their expectations of privacy.

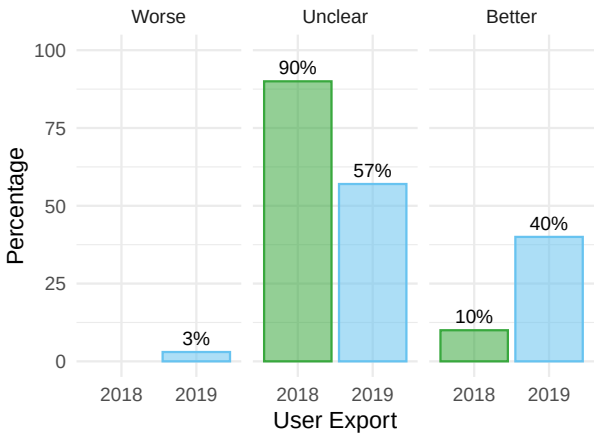


Figure 76: Do the policies clearly indicate whether or not a user can export or download their data, including any user-created content on the product?

Compared to 2018, applications and services evaluated in 2019 indicate a significant 29% increase in qualitatively better practices that companies disclose they allow users to export or download their data, including any user-created content on the product. In addition, since 2018 there has been a respective significant decrease of approximately 33%

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

163 California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(2).

164 General Data Protection Regulation (GDPR), Art. 13(2)(b), 14(2)(c), 20(1)-(2).

165 California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100(d), 1798.110(a)(1)-(5), 1798.130(a)(2).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

of unclear practices with companies increasing their transparency that they provide data export rights. Also, approximately 3% of applications and services disclosed qualitatively worse practices that users are not able to export or download their data, perhaps because these companies' policies restricted those rights only to verified EU citizens upon request.

Similarly to our analysis in the User Control section, this positive trend is likely the result of companies updating their policies for compliance purposes to incorporate new privacy rights granted by changing International and U.S. state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018, and provided many new privacy rights for companies subject to the GDPR's requirements with the ability for users to access, modify, and delete their personal information. Therefore, companies may be providing users with data export rights upon request for compliance purposes, but not disclosing their data export practices in their policies because they want to mitigate the high cost of compliance. Companies may also be concerned with "over-compliance," in particular by providing users a much larger data portability scope of personal and non-personal information collected under the GDPR than the CCPA, as described in the Usage Information section. In addition, companies may also not increase their transparency on this practice because it would increase consumer awareness of the right and the number of requests received. Lastly, to some extent, the exercise of this right may not be beneficial to a company, because users often only request to export or download their data when looking to leave the application and service for a better competitor.

Full: Data Sold

The concern of Data Sold addresses the practices of collecting personal information from users of an application or service in order to monetize that data through the disclosure of a user's personal information to a third-party company in exchange for monetary compensation based on the type and amount of information sold.

Data Sold Scores

Figure 77 illustrates the frequency of Data Sold scores among all applications and services evaluated. Table 19 compares and summarizes the Data Sold concern score minimum, maximum, median, mean, Q1 (point between the 1st and 2nd quartile), and Q3 (point between the 3rd and 4th quartile).

Table 19: 2018 vs. 2019 Data Sold score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	0	20	30	35	50	95
2019	0	25	35	40	55	95

From the analysis of 10 related questions in the concern, we determined a median in 2019 of approximately 35%. This median is lower than expected, given these applications and services are intended for children and students and 69% disclosed a qualitatively better response in the Data Sold section that they do not sell, rent, lease, or trade any users' personally identifiable information to third parties. However, several questions in this concern had relatively high percentages of unclear practices and approximately 80% disclosed a qualitatively worse practice in the Data Transfer section that collected information can be transferred to a successor third party in the event of a merger, acquisition, or bankruptcy.

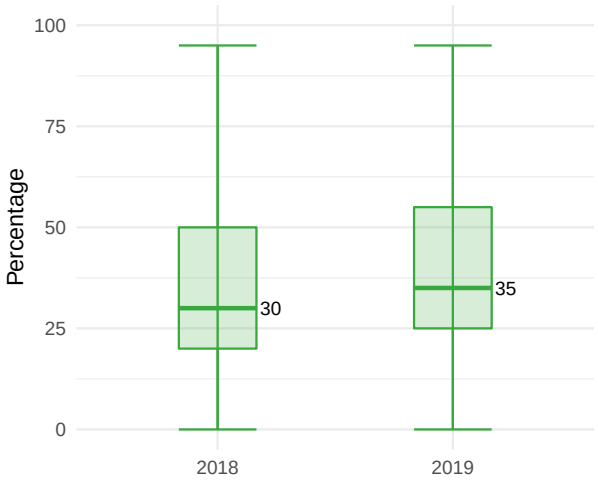


Figure 77: Comparison of Data Sold scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of Data Sold indicate a 16% increase in median scores that indicate more transparent and qualitatively better practices of not selling data to third parties. However, applications and services need to provide greater transparency on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students, but do not disclose whether they sell, rent, or lease collected personal information.

Data Sold

Among the applications and services we evaluated, approximately 69% 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 significant percentage, of approximately 29% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates a negligible percentage, of approximately 2% of applications and services evaluated discussed qualitatively worse practices that they sell, rent, lease, or trade users' personally identifiable information to third parties.

This unclear finding may be the result of applications and services choosing not to disclose practices they do not engage in, such as selling information collected from any users. However, companies with unclear terms often state in their policies that they make a distinction between personal information collected from parents or teachers, and personal information collected from children or students for commercial purposes. This practice of differentiating user data based on account type for commercial purposes is not considered a best practice, because it requires the application or service to embargo specific types of account data only after that user has logged into the service. Children's and students' personal information may still be inadvertently collected and sold to third parties before they log into the service and provide notice to the application or service that their information should be protected. Additionally, this type of practice if frowned upon as it makes navigating privacy issues more complicated for users, and users may change roles within the application based on details outside of their control such as their age. For these types of applications, a changing user role may mean different rules with respect to privacy and this present an unnecessary barrier to making an informed decision about a product. Moreover, because both Federal and State law clearly prohibit selling child and student data, we would like to assume that a large majority of unclear applications and services are in good faith following the law and not selling personal information to third parties, but are not disclosing compliance through their policies.[166,167,168]

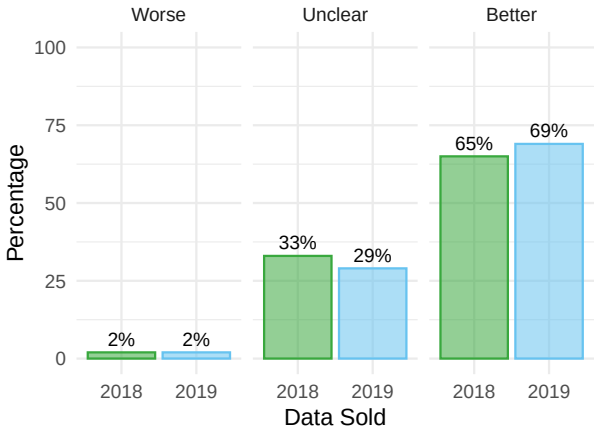


Figure 78: Do the policies clearly indicate whether or not a user's personal information is sold or rented to third parties?

Compared to 2018, applications and services evaluated in 2019 indicate a 4% increase in qualitatively better practices that companies disclose they do not sell, rent, lease, or trade any users' personally identifiable information to third parties. This positive trend is likely the result of selling data becoming one of the most controversial and widely known privacy practices among general consumers in 2018 with mainstream media headlines discussing Facebook's data misuse scandal with Cambridge Analytica, Europe's data General Data Protection Regulation (GDPR) prohibiting the sale of personal information without consent, and state legislation such as the California Consumer Privacy Act pushing for consumer's rights to opt out of the sale of their personal information to third parties.[169] In addition, the increase in better practices corresponds to a respective decrease of 5% of unclear practices in 2019 of selling data. This is an indication companies are updating their privacy policies with better practices to meet consumers' new expectations of privacy.

Applications and services need to provide greater transparency on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students, but do not also disclose whether they sell, rent, or lease collected personal information. When these practices are not 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.

166 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

167 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).

168 California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.115(a)(1)-(3), 1798.115(c)(1), 1798.120(c), 1798.135(a)(2)(A)-(B), 1798.140(t)(1).

169 *See* General Data Protection Regulation (GDPR), Art. 13(2)(b), 14(2)(c), 15(1)(e), 18(1)(d), 21(1), 21(4).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Opt-Out Consent

Among the applications and services we evaluated, approximately 55% disclosed a qualitatively better response that users can opt out from the disclosure or sale of their data to a third-party. However, our analysis indicates approximately 44% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates a negligible percentage of approximately 1% of applications and services evaluated discussed qualitatively worse practices that they do not allow users to opt out from the disclosure or sale of their data to a third-party.

Given that 96% of companies, as indicated in the Data Shared section, disclose they share data with third parties we would expect a higher percentage of applications providing opt-out privacy protections. Unfortunately, we still see a large percentage (44%) of applications and services that are unclear with respect to any additional user protections to mitigate the sharing or selling of their data. Optimistically, it may be that some of the more privacy aware applications and services are providing opt-in consent and we do not currently capture those details or practices.

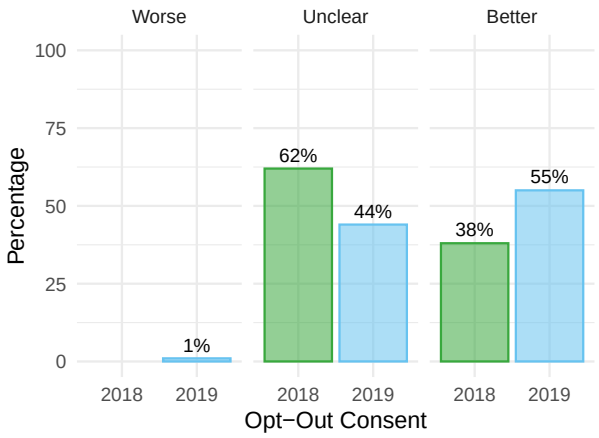


Figure 79: Do the policies clearly indicate whether or not a user can opt out from the disclosure or sale of their data to a third party?

Compared to 2018, applications and services evaluated in 2019 indicate a 17% increase in qualitatively better practices that users can opt out from the disclosure or sale of their data to a third-party. This positive trend is likely the result of the issue of "opting-out" from a company selling a consumer's data becoming a more widely known privacy practice that consumers can exercise to protect their personal information. Also, in 2018, there was an increased consumer awareness of privacy with mainstream media headlines discussing Facebook's data misuse scandal with Cambridge Analytica, and Europe's General Data Protection Regulation (GDPR) that allows data subjects to withdraw consent or object to the sale of their personal information, and U.S state legislation such as the California Consumer Privacy Act (CCPA) that provides consumers with the right to opt out of the sale of their personal information to third parties.[170,171,172,173,174] Therefore, companies likely updated their policies both for compliance purposes and in response to consumer demand to provide them with the ability to exercise their privacy rights to opt out from the sale of their data to third parties.

However, applications and services need to provide greater transparency on this issue, because although there was an 18% decrease in unclear disclosures, approximately 44% are still unclear on the issue of opt-out consent. These products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students, but do 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.

Transfer Data

Among the applications and services we evaluated, approximately 81% 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. However, our analysis indicates approximately 17% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates a negligible percentage of approximately 2% of applications and services evaluated discussed qualitatively better practices that personal information will not be transferred as an asset to a successor third party in the event of a merger, acquisition, or bankruptcy.

This qualitatively worse finding of the vast majority of companies engaging in this practice is the result of companies established practices of seeking to monetize a company's assets including users' personal information, in the event of a merger, acquisition, or bankruptcy. However, 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

170 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.3, 99.37.

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

172 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(5).

173 California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.115(d), 1798.120(a), 1798.135(a)-(b), 1798.135(a)(1).

174 *See* General Data Protection Regulation (GDPR), Art. 7(3), 13(2)(b), 14(2)(c), 15(1)(e), 21(1), 21(4).

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 of privacy risks and harms. 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 practice can be mitigated however, as illustrated in our analysis of Collection Limitation, where approximately 66% 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 in which to transfer to third parties. Moreover, many companies that transfer data to third parties are unclear or do not mitigate this practice by providing Transfer Notice to users of the forthcoming merger, acquisition, or bankruptcy and requiring Contractual Limits on successor companies to adopt the company's privacy policy and privacy practices at the time of transfer.

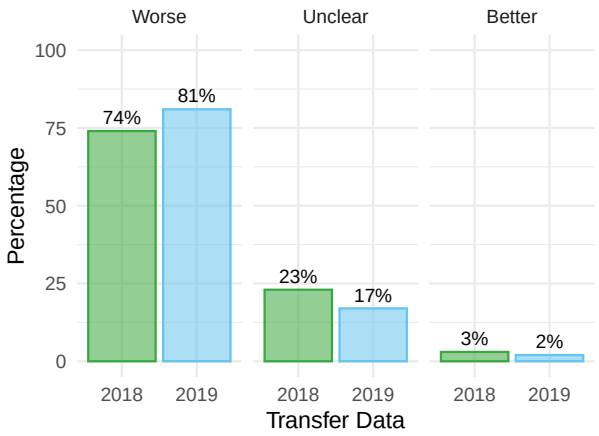


Figure 80: Do the policies clearly indicate whether or not the vendor can transfer a user's data in the event of the vendor's merger, acquisition, or bankruptcy?

Compared to 2018, applications and services evaluated in 2019 indicate a 7% decrease in unclear disclosures and respective 6% increase in qualitatively worse practices that collected information can be transferred to a successor third party in the event of a merger, acquisition, or bankruptcy. This negative trend may be the result of companies updating their policies in 2018 to be more transparent for compliance purposes.[175,176] However, approximately 17% of applications and services are nontransparent 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% of applications and services may transfer collected information in this context, and in many cases may transfer information without contractual limitations or obligations on the third party recipient.[177,178]

In addition, as indicated in the Contractual Limits section, many applications and services are unclear 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 and delete their personal information before it is transferred to a third party. Therefore, third parties can still use and disclose transferred information in an anonymous or deidentified 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 different context from which it was collected.

Transfer Notice

Among the applications and services we evaluated, approximately 67% did not disclose whether or not the company will notify users of a data transfer to a third-party successor, in the event of a vendor's bankruptcy, merger, or acquisition. However, our analysis indicates approximately 30% of applications and services discussed qualitatively better practices on this issue. In addition, our analysis indicates a negligible percentage of approximately 3% of applications and services disclosed a qualitatively worse practice that they will not provide notice in the event of a vendor's bankruptcy, merger, or acquisition.

This unclear finding may be companies assuming that collected personal information from users of their applications and services are considered assets of the company that can be monetized with all the other assets of a company in the event of a vendor's bankruptcy, merger, or acquisition.[179] For example, in 2018, the Chinese company NetDragon acquired a popular edtech product called Edmodo. During that acquisition, Edmodo transferred ownership of

175 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

176 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).

177 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(t)(2)(D).

178 *See* General Data Protection Regulation (GDPR), General principle for transfers, Art. 44.

179 *See* General Data Protection Regulation (GDPR), Art. 13(1)(f), 14(1)(f), 15(2).

its assets which included users' personal information.[180] Acquisition of companies by other companies under different International jurisdictions presents additional legal complications when navigating privacy concerns especially with respect to the transfer of data. There are additional concerns with regard to foreign state interception and access to information of U.S. users if the data is collected or stored in another country. Providing notice to users in the event of a bankruptcy, merger, or acquisition allows users to exercise their choice to continue using that application or service if the privacy practices that govern the collection and use of their personal information are expected to change.

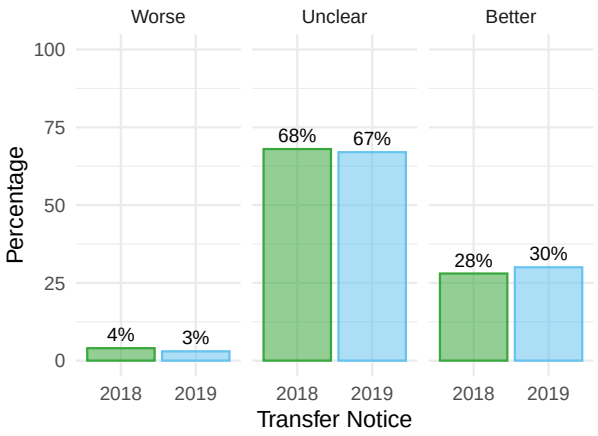


Figure 81: Do the policies clearly indicate whether or not the vendor will notify users of a data transfer to a third-party successor, in the event of a vendor's bankruptcy, merger, or acquisition?

Compared to 2018, applications and services evaluated in 2019 indicate a negligible 1% decrease in unclear practices, and a respective 1% increase in qualitatively better and worse practices about whether the company will notify users of a data transfer to a third-party successor, in the event of a vendor's bankruptcy, merger, or acquisition. Low awareness among parents and teachers, as can be seen by these applications and services being among the most used edtech products, combined with companies that put a low value on this issue of notice and choice for users to exercise their privacy rights in the event of a bankruptcy, merger, or acquisition are the likely reasons for this plateau in industry norms.

From our analysis, it appears there is a disproportionate percentage of an approximately 51% higher occurrence in the disclosure of qualitatively worse practices that a company may Transfer Data (81%) in the event of a bankruptcy, merger, or acquisition, as compared to the percentage of companies (30%) that also disclose they provide Transfer Notice in the event data will be transferred. Therefore, at least half of all companies that disclose they may transfer a user's data to third parties in the event of a bankruptcy, merger, or acquisition do not also disclose they provide notice to those same users so they may exercise their privacy rights.

Delete Transfer

Among the applications and services we evaluated, approximately 19% disclosed a qualitatively better response that 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. However, our analysis indicates approximately 78% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately only 3% of applications and services evaluated discussed qualitatively worse practices that they do not allow a user to delete their data prior to its transfer to a third-party successor in the event of a vendor bankruptcy, merger, or acquisition.

Similarly to our analysis of Transfer Notice, the finding that a majority of applications and services are unclear on this issue may be the result of a company's assumption that collected personal information from users of their applications and services are considered assets of the company that can be monetized with all the other assets of a company in the event of a vendor's bankruptcy, merger, or acquisition. Providing notice to users of their rights to delete their personal information or account in the event of a bankruptcy, merger, or acquisition allows users to make an informed choice to continue using that application or service or delete their account and leave if the privacy practices that govern the collection and use of their personal information are expected to change.[181] This lack of transparency and user agency is notable given that, as seen in User Deletion, 66% of applications and services indicate that a user may delete personal and non-personal information. It may be that some of these vendors do intend to allow users to delete data in the event of a bankruptcy, merger, or acquisition but have not clarified this intent in their policies.

[180] Corcoran, B., and Wan, T., *China's NetDragon to Acquire Edmodo for $137.5 Million*, Edsuge (Apr. 9, 2018), https://www.edsurge.com/news/2018-04-09-china-s-netdragon-to-acquire-edmodo-for-137-5-million.

[181] *See* General Data Protection Regulation (GDPR), Right to erasure, Art. 17(1),17(1)(a)-(c).

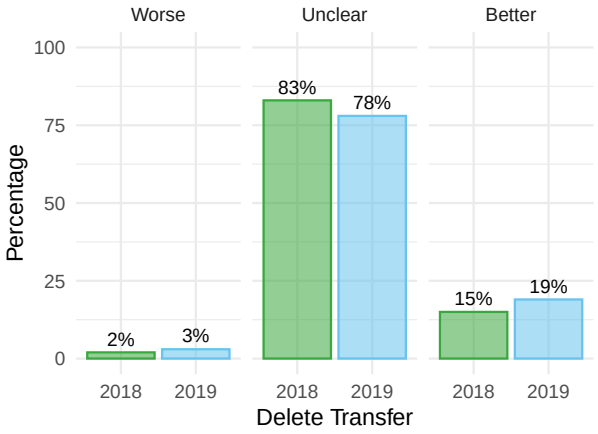


Figure 82: Do the policies clearly indicate whether or not a user can request to delete their data prior to its transfer to a third-party successor in the event of a vendor bankruptcy, merger, or acquisition?

Compared to 2018, applications and services evaluated in 2019 indicate a 5% decrease in unclear practices and respective 4% increase in qualitatively better practices that companies disclose they allow a user to delete their data prior to its transfer to a third-party successor in the event of a vendor bankruptcy, merger, or acquisition. This positive trend is may be the result of greater awareness about this issue by companies that updated their policies in 2018 to include additional disclosures that users may request to access, modify, and delete their personal information. The high percentage of unclear responses may be because the ability for users to exercise their rights to delete their personal information or account on the application or service is assumed to be the same practice by vendors as the right of a user to delete personal information in the event of a bankruptcy, merger, or acquisition.

However, from our analysis it appears there is disproportionate percentage of an approximately 62% higher occurrence in the disclosure of qualitatively worse practices that a company may Transfer Data (81%) in the event of a bankruptcy, merger, or acquisition, as compared to the percentage of companies (19%) that also disclose they provide users the ability to delete their data in the event data will be transferred. Therefore, at least half of all companies that disclose that they may transfer a user's data to third parties in the event of a bankruptcy, merger, or acquisition do not also disclose they allow users to exercise their privacy rights to delete their data in the event of a transfer.

Contractual Limits

Among the applications and services we evaluated, approximately 48% disclosed a qualitatively better response that the third-party successor of a data transfer is contractually required to provide the same privacy compliance required of the vendor. However, our analysis indicates approximately 51% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 1% of applications and services evaluated discussed qualitatively worse practices that the third-party successor of a data transfer is not contractually required to provide the same privacy compliance required of the vendor.

This unclear finding may be the result of approximately 70% of companies already disclosing they require contractual restrictions on any third-party service providers in which they share personal information, as described in our analysis of Third-Party Limits. However, a company may transfer a child or student's personal information to a third party in the event of a merger, acquisition, or bankruptcy, but the policies should disclose that any successor entity is subject to the same or better onward data privacy and security obligations as the company's existing privacy policies.[182,183,184]

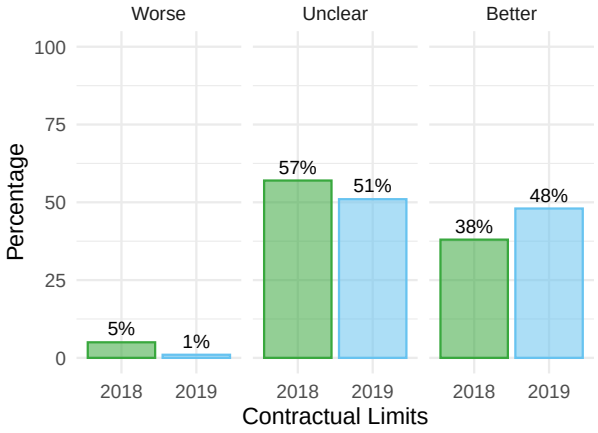


Figure 83: Do the policies clearly indicate whether or not the third-party successor of a data transfer is contractually required to provide the same privacy compliance required of the vendor?

Compared to 2018, applications and services evaluated in 2019 indicate a 9% increase in qualitatively better practices that in the event of a data transfer the acquiring third-party is contractually required to provide the same privacy protections established by the vendor. In addition, since 2018, nontransparent disclosures decreased 6% and qualitatively worse practices decreased 4%. This positive trend may be the indirect result of companies updating their policies to disclose they may engage in the qualitatively worse practice of transferring data in the event of a bankruptcy, merger,

182 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.
183 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).
184 *See* General Data Protection Regulation (GDPR), General principle for transfers, Art. 44.

or acquisition, but also mitigating that practice by providing additional obligations on third parties and rights for users related to the transfer of their data, as described with Transfer Notice and Delete Transfer.

Data Deidentified

Among the applications or services we evaluated, approximately 55% disclosed that the application or service shares information with third parties in an anonymous or deidentified format. However, our analysis indicates approximately 29% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 16% of applications and services evaluated disclosed they do not share information with third parties in an anonymous or deidentified format.

The practice of sharing deidentified information is an important exception to the general prohibition on sharing child or student personal information with unaffiliated third parties. As compared to Data Shared, there is a difference of approximately 42% of applications and services that disclose they share data with third parties, and those that disclose collected information is shared in an anonymous or deidentified format. Sharing collected information in an anonymous or deidentified format is a complicated issue and even data that has gone through this process can be often be recombined with other data to allow re-identification. As such, sharing of any information, even information about a user that has been deidentified or anonymized, is a privacy risk.

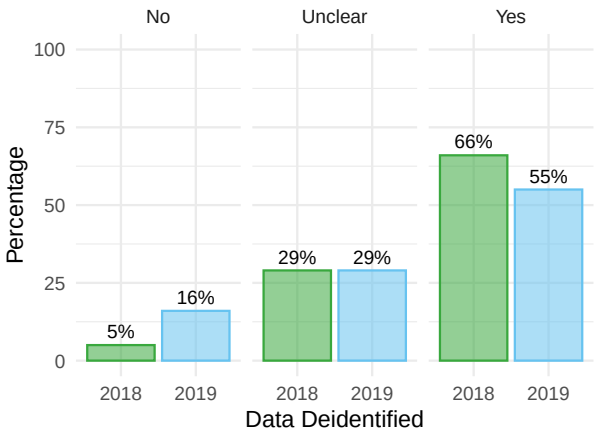


Figure 84: Do the policies clearly indicate whether or not a user's information that is shared or sold to a third party is only done so in an anonymous or deidentified format?

Compared to 2018, applications and services evaluated in 2019 indicate an 11% decrease in companies that share information with third parties in an anonymous or deidentified format. In addition, compared to 2018 there is an 11% increase in companies that do not share information with third parties in an anonymous or deidentified format. However, as seen in the Data Shared section, roughly 96% of applications and services are sharing data with third parties. Given the difficulty in successfully deidentifying data we would expect more than 12% of applications and services to disclose that they require Combination Limits when sharing data to third parties in a deidentified format. However, a small percentage of companies that share deidentified data with third parties but do not disclose that they require combination limits may be because they require additional contractual agreements with combination limits that prohibit third parties from re-identifying or combining data with other data sources.

However, approximately 29% of applications and services evaluated were nontransparent on this issue, possibly because they do not share child or student data in anonymized or deidentified formats for non-educational purposes and do not disclose practices they do not otherwise engage in. Disclosing how information is shared with third parties provides parents and teachers with more information in order to make an informed decision about whether to use an application or service, and is a critical issue for vendors to disclose in order to remain in compliance when sharing data with third parties for non-educational purposes.[185,186,187,188,189,190] Given the complexity of deidentification, it should be seen as a last-resort mitigation technique and only when appropriate Combination Limits are combined with a robust Deidentified Process. Lastly, the finding that companies disclose that they do not share personal information with third parties in an anonymous or deidentified format may be because some of their policies typically define a broader range of company partners, affiliates, and transactional companies in which they share only personal information.

Deidentified Process

Among the applications and services we evaluated, approximately 19% disclosed a qualitatively better response that any deidentification process is done with a reasonable level of justified confidence, or the vendor provides links to any information that describes their deidentification process. However, our analysis indicates a majority, approximately 81% of applications and services evaluated, are unclear on this issue. In addition, our analysis indicates zero percent of applications and services evaluated in both 2018 and 2019

185 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
186 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(b)(1).
187 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(f)-(g).
188 California Privacy of Pupil Records, Cal. Ed. Code § 49074.
189 California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.140(a), (h), (r); 1798.145(a)(5).
190 *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(5), 25(1).

disclosed qualitatively worse practices that any deidentification process is not completed with a reasonable level of justified confidence, which is expected.

That said, deidentification is a very complicated subject and "a reasonable level of justified confidence" is a broad term for an area where big data can often provide surprising results. For instance, the combination of zip code, birth data, and gender is enough data to uniquely identify 63% of the U.S. population using 2000 census data.[191] In addition, simply collecting demographic attributes without Combination Limits makes any deidentification process largely ineffective.[192] This lack of transparency is the result of companies not disclosing their deidentification or anonymization process beyond general statements that they remove personal information, which is not sufficient to properly describe their deidentification or anonymization process. Companies are required to disclose that their deidentification or anonymization of personal information is completed in a manner such that personal data can no longer be attributed to a specific individual without the use of additional information.[193,194] In addition, the company should describe or provide links to any technical and organizational measures they use to ensure that the personal data of their users are not attributed to a specific individual. However, approximately 19% of applications and services indicate justified confidence or describe their deidentification or anonymization process to protect personal information pertaining to children or students.

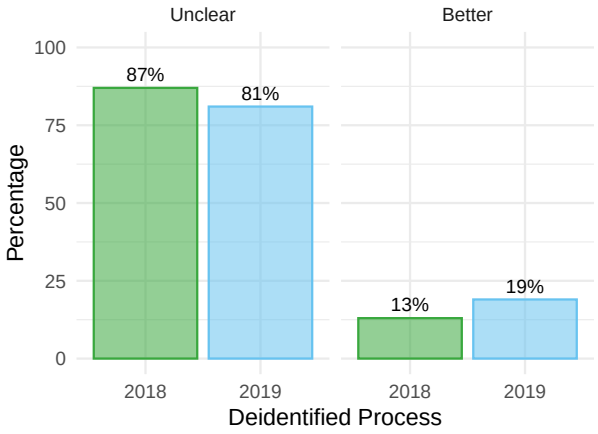


Figure 85: Do the policies clearly indicate whether or not the deidentification process is done with a reasonable level of justified confidence, or the vendor provides links to any information that describes their deidentification process?

Compared to 2018, applications and services evaluated in 2019 indicate a 6% increase in qualitatively better practices that companies disclose any deidentification process is done with a reasonable level of justified confidence, or the vendor provides links to any information that describes their deidentification process. In addition, since 2018, there was a respective decrease in unclear practices of approximately 7%.

This positive trend may be the result of an increased awareness in 2019 by companies of the complexity of sharing personal information with third parties in a deidentified or anonymized format that cannot be easily used to re-identify a specific individual. As discussed in the Data Deidentified section, more companies are disclosing they do not share deidentified data with third parties since 2018. Accordingly, companies may be including additional disclosures on the technical and organizational measures they use to ensure that the personal data of their users are not attributed to any specific individual, so they can still use the data internally for their own product development and compliance purposes.

Third-Party Research

Among the applications and services we evaluated, approximately 6% disclosed a qualitatively better response that collected information is not shared with third parties for their research or product-improvement purposes. However, our analysis indicates approximately 43% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 51% of applications and services evaluated discussed qualitatively worse practices that they may share information with third parties for their research or product-improvement purposes.

This qualitatively worse finding is likely the result of companies monetizing and/or analyzing collected usage or behav-

191 Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population*, Proceedings of the 5th ACM workshop on Privacy in electronic society, pp. 77-80 (October 30, 2006), https://doi.org/10.1145/1179601.1179615.

192 Rocher, L., Hendrickx, J. M., de Montjoye, Y., *Estimating the success of re-identifications in incomplete datasets using generative models*, Nature Communications, vol. 10, art. 3069 (Jul. 23, 2019), https://doi.org/10.1038/s41467-019-10933-3.

193 *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(h)(1)-(4).

194 General Data Protection Regulation (GDPR), Definitions, Art. 4(5).

ioral information of applications and services with third parties but only in a deidentified or anonymized format. However, companies can mitigate these risks by deidentifying or anonymizing children's and student's personal information before sharing with a third party company or research institution and placing contractual limits on those companies of their use of the data, as described in the Data Deidentified and Third-Party Limits sections. Companies often share this information under compliance exceptions to sharing data, to third-party companies or university research institutions for behavioral research purposes on how children, or how students use particular types of applications or services in order to better understand how to improve an application, and/or the service's learning potential and efficacy.[195,196,197,198,199,200] In addition, behavioral information is also shared with third parties for product development purposes to build better products that take advantage of particular positive outcomes or benefits of children or students using the product. However, this practice disproportionately impacts children and students using free or low-cost applications and services because these easier to procure products may be subsidizing the cost of these technologies through third-party research in order to increase adoption and they may implement greater data collection through personalized learning technologies. This practice can serve to monetize users' behavioral information using the application or service by disclosing it to third parties to build better products. Unfortunately, this practice allows companies to create more expensive and robust featured technologies based on the research findings of low-income children and students that may not benefit from their contributions. Furthermore, a large percentage of companies with unclear disclosures in their policies may be engaging in the practice of sharing deidentified or anonymized behavioral information of users with third parties, but are not choosing not to disclose the practice in their policy because there is no compliance-related obligations despite limitations of deidentification processes.

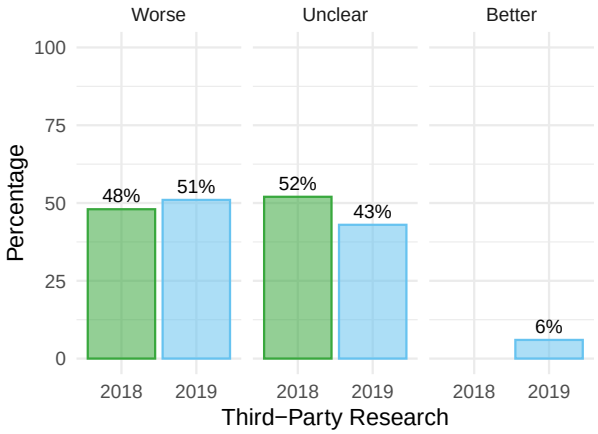


Figure 86: Do the policies clearly indicate whether or not collected information is shared with third parties for research or product improvement purposes?

Compared to 2018, applications and services evaluated in 2019 indicate a 6% increase in companies that do not share collected information with third parties for their research or product-improvement purposes. This positive trend is likely the result of increased awareness among parents and educators of the practice of third-party research and data misuse in 2018. This increased awareness was due to mainstream media headlines discussing Facebook's data misuse scandal with a third-party research and data analysis company Cambridge Analytica. The 10% decrease in nontransparent policies and relative 6% increase in qualitatively better disclosures indicates companies becoming more aware of this issue and either adjusting practices to not share data with third parties for research purposes, or clarifying already existing practices. Clarifying policies on popular and emerging concerns is an excellent way for privacy-forward companies to differentiate their products and respond to parents' and educators' privacy expectations. However, most applications and services need to provide greater transparency on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students, but do not also disclose whether collected information is not shared with third parties for their research or product-improvement purposes.

Combination Limits

Among the applications and services we evaluated, approximately 12% disclosed that they impose contractual limits that prohibit third parties from re-identifying or combining data with other data sources that the company shares or sells to them. However, our analysis indicates the majority, approximately 86% of applications and services evaluated, are unclear on this issue. In addition, our analysis indicates

195 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
196 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.31(a)(6), 99.31(b)(2).
197 Protection of Pupil Rights Act (PPRA), 34 C.F.R. §98.3.
198 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(e)(2), 22584(b)(4), 22584(l).
199 California Privacy of Pupil Records, Cal. Ed. Code § 49074.
200 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(s)(1)-(2), (7)-(9).

approximately 2% of applications and services evaluated discussed qualitatively worse practices that there are no contractual limits that prohibit third parties from re-identifying or combining data with other data sources that the company shares or sells to them.

This lack of transparency is likely the result of companies that are unaware that they need to disclose that any data they share with third parties cannot be used to re-identify specific users, which would render any deidentification process irrelevant or be a different use than what the company intended when sharing data. In addition, our analysis in the Contractual Limits section indicates approximately 71% of applications and services disclose they impose contractual limits on how third parties can use personal information that the company shares or sells to them. However, these contractual limits on third parties are often only limited to the scope of the company's privacy policy, which often does not include re-identification or data combination restrictions that could be applied to third parties.[201,202] Our analysis in the Combination Type section indicates only approximately 27% of applications and services disclose that if they combine personal information with data from other sources that they will treat the combined data as protected personal information.

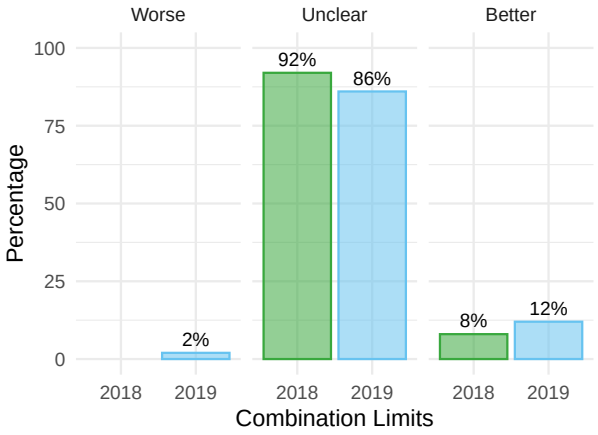


Figure 87: Do the policies clearly indicate whether or not the vendor imposes contractual limits that prohibit third parties from re-identifying or combining data with other data sources that the vendor shares or sells to them?

Compared to 2018, applications and services evaluated in 2019 indicate a 4% increase in qualitatively better practices that companies disclose they impose contractual limits that prohibit third parties from re-identifying or combining data with other data sources that the company shares or sells to them. This positive trend may be the result of increased awareness of the power of big data and the potential for misuse of data. If a company discloses student information to a third party service provider, the third party should be prohibited from using the information for or any purpose other than providing the service. However, in addition to placing contractual restrictions on third parties, companies should also disclose they place restrictions on the re-identification of information shared with third parties because it prevents potential data misuse by the third party and mitigates the risk of the onward transfer of that information to other companies. Also, restrictions on third-party re-identification can act to maintain data in a deidentified or anonymized format which protects against the identification of specific users' personal information in the event of a data breach by a third party provider. However, the act of sharing data is still an inherently risky behavior because even with policies and contractual obligations in place, data breaches are a very real threat.

[201] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.8.

[202] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(s)(3)-(6).

Full: Data Safety

The concern of Safety primarily examines practices where children or students' information could be made publicly visible to others, and where social interactions with other children or strangers are made available.

Data Safety Scores

Figure 88 illustrates the Data Safety scores among all applications and services evaluated. Table 20 compares and summarizes the Data Safety concern score minimum, maximum, median, mean, Q1 (point between the 1st and 2nd quartile), and Q3 (point between the 3rd and 4th quartile).

Table 20: 2018 vs. 2019 Data Safety score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	0	5	22	26	40	90
2019	0	15	40	36	55	90

From the analysis of 10 related questions in the concern, we determined a median in 2019 of approximately 40%.

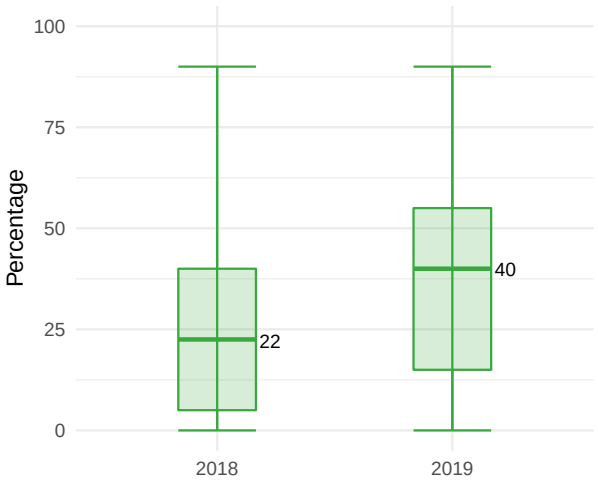


Figure 88: Comparison of Data Safety scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of Data Safety indicate a 45% increase in median scores which is the largest positive increase across all our concerns. This significant increase indicates more transparent and qualitatively better practices that protect the safety of children and students when the application or service provides social interaction features. The industry has significantly improved its practices regarding Data Safety as seen by the 2019 median equalling Q3 of 2018 for the concern of Data Safety.

However, even with such a significant improvement since 2018 this median is still considerably lower than expected, given these applications and services are intended for children and students and a majority of companies disclose qualitatively better practices that they provide safe interactions and limit public visibility of personal information. Many applications and services do not allow children or students to make personal or non-personal information visible, or provide any social interactions with others. As such, these services are not likely to disclose information about safety features for controls related to functionality they do not provide. Additionally, applications and services may be unaware they should provide clarification in their policies about common safety risks, such as children or students making personal information visible, or providing social interactions with strangers. Even when an application does not directly collect personally identifiable information, allowing children and students to enter text in any field or upload files may result in unintended sharing of personal information. Additionally, applications and services may be unaware that even if they do not provide these features they should still provide notice in their policies that these types of interactions or risks are not present on their application or service.

This lower median score is also likely attributable to the fact that most applications and services that are transparent about safety also disclose qualitatively worse safety practices. For example, a company's disclosures are more likely to be qualitatively worse, because features relating to visibility of information and communications with others inherently places children and students' information more at risk. In addition, there is an increased risk for 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 scores between applications or services that may have differing safety protections depending on the type of user account. For example, parent or teacher restrictions on what data can be made available for adults and restrictions on which individuals a child or student can communicate with are not reflected in the Data Safety concern score. Therefore, our evaluation process indicates that applications or services that simply provide any of these features would receive a lower score, with the expectation that parents, teachers, schools, and districts should learn more about what safety protections or controls are in place for all intended users of a product to help mitigate these risks. Lastly, these features are important differentiating factors for parents, teachers, schools, and districts when choosing between applications or services, and companies are recommended to increase their transparency on these important safety issues.

Safe Interactions

Among the applications and services we evaluated, approximately 61% disclosed that users can interact with trusted users. However, our analysis indicates approximately 36% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 3% of applications and services evaluated disclosed that users cannot interact with trusted users.

Schools and educators have always been concerned with interactions of all kinds for their students. They are responsible for communications between their students and interactions between their students and school staff. They are also concerned about interactions that their students have with individuals outside of the school setting. With the prevalence of communication technology in schools, these concerns are amplified as connected students have the capacity for interactions with many different types of people. Safe interactions represent the ability for children or students using an application or service to only interact with other trusted users such as friends they know and trust or other students in the same class. Depending on the context, safe interactions could be with other students in the same classroom, grade, or school, or between students and their teacher, or could also include a parental contact. Is important to note

that the capability for safe interactions does not preclude the opportunity for interactions with untrusted individuals or strangers, as discussed in the Unsafe Interactions section. Since communication features are often an important part of technology interactions in a school setting, this is an important practice that vendors should disclose in policies.[203]

The unclear finding for safe interactions may be the result of applications and services that do not include social interaction related features in their products that would allow children or students to make personal or non-personal information visible, or to communicate with others. These applications and services are not likely to disclose information about social interaction features or controls they do not otherwise provide. Additionally, applications and services may be unaware that even if they do not provide these features they should still provide notice in their policies that these types of interactions or risks are not present on their application or service. Therefore, if a vendor is not transparent on this issue in their policy than it must be assumed that social interactions may be possible, whether safe or unsafe.

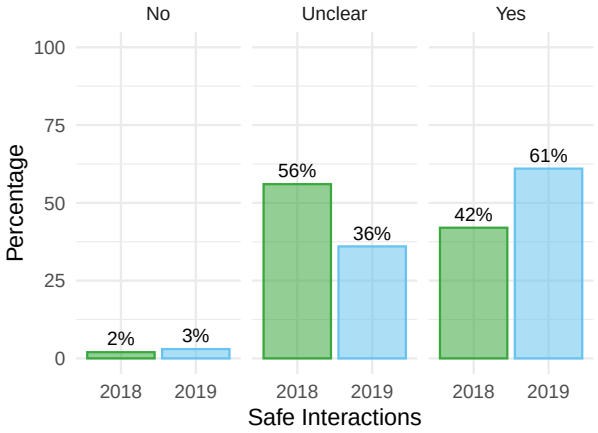


Figure 89: Do the policies clearly indicate whether or not a user can interact with trusted users?

Compared to 2018, applications and services evaluated in 2019 indicate a 19% increase in transparent practices that companies disclose users can interact with trusted users. In addition, there was also a corresponding decrease of 20% in unclear responses. This positive trend is likely the result of increased awareness of the safety risks inherent in social interactions with trusted and untrusted individuals. The 19% increase in transparent practices and 20% reduction in unclear responses is trending in the right direction, although this still leaves approximately 36% with unclear practices. Since the safety of interactions with children is such a critical issue for parents and educators, it is recommended that all vendors clearly disclose whether or not their product provides social interactions and if those interactions are with trusted or untrusted individuals.

Unsafe Interactions

Among the applications or services we evaluated, approximately 19% disclosed interactions are not available with untrusted users. However, our analysis indicates approximately 39% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 42% of applications and services evaluated disclosed that users can interact with untrusted users.

This qualitatively better finding is lower than expected, perhaps because most applications or services evaluated that have social interaction features have already disclosed they provide safe interactions between children and students in their policies, as described in the Safe Interactions section, and therefore do not believe they also need to disclose whether or not they provide unsafe interaction features as well. In addition, vendors may assume applications and services that disclose they are intended for a general audience and not children or students allow social interactions with untrusted users as a primary feature, and therefore they do not need to disclose unsafe interactions in their policies. This unexpectedly low qualitatively better percentage may also be attributable to vendors mitigating this issue, as discussed in the Moderating Interactions section. As a result, we assume among the approximately 39% of unclear responses to this question that otherwise provide safe interactions, there is likely a small percentage that have qualitatively better practices, but do not disclose whether those restrictions or controls are in place by default. In contrast, approximately 42% of applications and services disclosed that social interactions can occur between children or students with untrusted users including strangers or adults; practices which may be in violation of Federal law if appropriate protections are not put in place.[204]

From our analysis, applications and services with social interaction features often provide unmoderated chat rooms, forums, open text fields, and comment areas. These features are typically provided to children and students without sufficient safety protections or controls in place. Therefore, it is recommended that vendors increase their transparency on this important safety issue and put stronger protections and controls in place by default to help parents, teachers, schools, and districts to help mitigate unsafe interactions.

[203] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.4(d)(2).

[204] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.4(d)(2).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

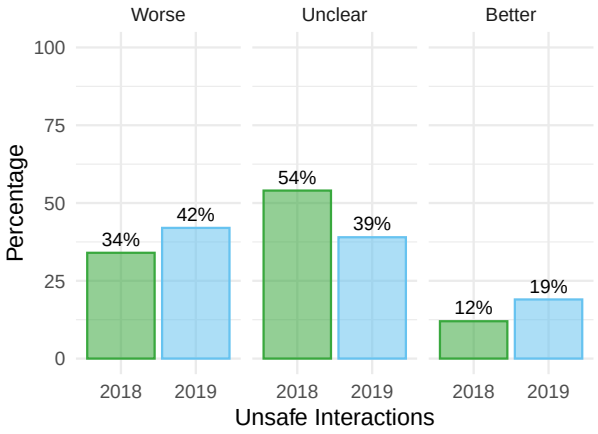


Figure 90: Do the policies clearly indicate whether or not a user can interact with untrusted users?

Compared to 2018, applications and services evaluated in 2019 indicate a 7% increase in qualitatively better practices that children and students cannot interact with untrusted users. In addition, since 2018, our findings indicate unclear practices decreased 15% and there was a respective 8% increase in qualitatively worse practices that children and students can interact with untrusted users. Although there is a higher percentage of applications or services that disclose they provide unsafe intersections since 2018, the overall increase in transparency of this information makes it possible for parents and educators to make a more informed decision as to whether or not the application or service should be used based on context.

Only 19% of applications and services disclose better practices for this issue. However, when comparing to Children Intended responses, where approximately 68% disclosed products are intended for children there is at least a 49% difference in products that are intended for children, but do not also disclose that interactions with untrusted users are not permitted. Given these products are among the 150 most popular educational technology products and unsafe interactions is a special concern for children, this would suggest that vendors need to update their policies to disclose this practice to better assist parents and educators in deciding which products to use with children. Therefore, applications and services need to disclose better practices on this issue, because these products are among the most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students, but do not also disclose whether they provide safe or unsafe interactions.

Share Profile

Among the applications and services we evaluated, approximately 13% disclosed a qualitatively better response that profile information is not required to be shared or revealed by a user in order to participate in social interactions. However, our analysis indicates approximately 42% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 45% of applications and services evaluated discussed qualitatively worse practices that information must be shared or revealed by a user in order to participate in social interactions.

With increased interest in single sign-on accounts and other forms of social login services, as discussed in the Social Login section, profile visibility is becoming an increasingly important issue, especially where children and students are concerned. Where social interactions are possible, vendors need to clearly state in their policies what information is required to be shared in order to communicate with trusted and untrusted users, as discussed in the Safe Interactions and Unsafe Interactions sections. Parents and educators expect to know before using a product if it provides features that allow their children or students to communicate with other children or student users anonymously, or if personal profile information must be shared to participate. If profile information is shared in order to communicate or collaborate with others—in the case of children under the age of 13—this could present possible COPPA violations if shared publicly and, for older children, there are additional compliance considerations.[205]

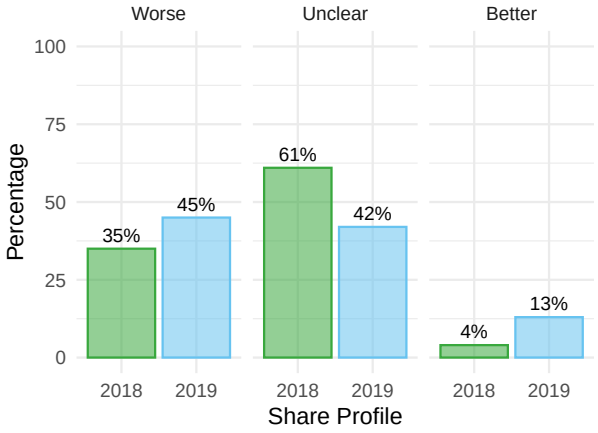


Figure 91: Do the policies clearly indicate whether or not information must be shared or revealed by a user in order to participate in social interactions?

Compared to 2018, applications and services evaluated in 2019 indicate a 9% increase in qualitatively better practices that profile information is not required to be shared or revealed by a user in order to participate in social interactions. In addition, since 2018, there has been a 19% decrease in unclear practices, but also a 10% increase in qualitatively

[205] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(2).

worse practices. This increase in qualitatively better practices may be the result of increased adoption of single sign-on accounts, as discussed in the Social Login section, and vendors updating their policies to clarify their safety practices with these new social interaction features that include limiting public visibility of users' profile information. School districts are also increasingly concerned about more student communication features in popular edtech products and are looking to increase oversight of social interactions and sharing of personal information, as discussed in the Managed Account section.

Since 42% of applications and services, as indicated in the Unsafe Interactions section, allow interactions with untrusted users, we would expect more than 13% of applications and services to allow interactions without sharing profile information. Therefore, it is recommended that vendors increase their transparency on this important issue of requiring children and students to share profile information in order to engage in social interactions. If social interactions are available to children and students, it is recommended that they be able to participate with pseudonyms or without displaying any more personal information than necessary to use the product.

Visible Data

Among the applications or services we evaluated, approximately 19% disclosed a qualitatively better response that no personal information can be displayed publicly. However, our analysis indicates approximately 34% of applications and services evaluated are unclear on this issue. In addition, approximately 47% of applications and services disclose qualitatively worse practices that children or student's information can be made publicly visible.

Similarly to the Unsafe Interactions section, this finding is not surprising, as many applications or services evaluated are unclear about this issue. Of the 34% of unclear responses to this question there is likely a significant percentage that have otherwise qualitatively better practices, but do not disclose what those practices are. The practice of making personal information of children and students publicly available online exposes them to privacy risks and harms such as inappropriate contact from strangers or child groomers, that could pose direct physical and safety concerns. Offenders often begin grooming child victims on platforms where their profile information is publicly accessible to all the other users of the service, or available to the general public without an account. These "bad actors" gain a child or student's attention or trust, before moving the communication off the edtech application or service to another video- and photo-sharing platform, which can lead to content-driven or financially driven extortion or meeting offline. Therefore, parents and teachers need to exercise caution when evaluating whether to use popular edtech applications with features that allow children or students to share information publicly with others, and vendors need to provide greater transparency on this critical 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.[206].

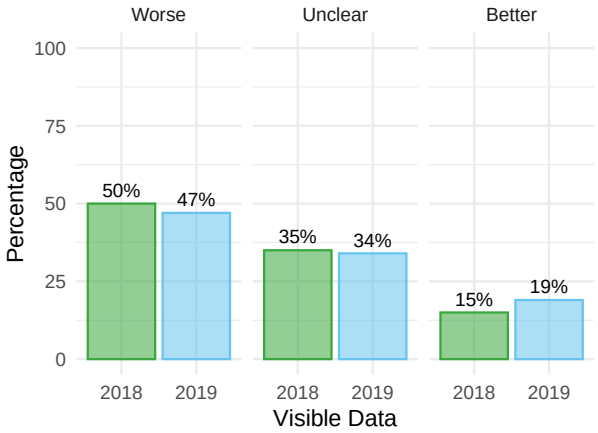


Figure 92: Do the policies clearly indicate whether or not a user's personal information can be displayed publicly in any way?

Compared to 2018, applications and services evaluated in 2019 indicate a 4% increase in qualitatively better practices that personal information cannot be publicly displayed. In addition, since 2018 there is also a 3% decrease in qualitatively worse practices that personal information can be publicly displayed. This slight shift towards qualitatively better practices may be the result of increased school and district concern for student personal information being displayed publicly.

From our analysis, it appears there is approximately a 6% lower occurrence in the disclosure of qualitatively worse practices that personal information can be publicly displayed (47%), as compared to the Control Visibility section that discloses qualitatively better practices (53%) that controls are available to limit public visibility of personal information. This may indicate vendors are attempting to mitigate allowing personal information to be made publicly available by also allowing users to control which data is publicly visible and which data is private. However, it is recommended that an application's or service's privacy controls are set by default to their most privacy-restricting settings, which allows for user notice and informed consent to change a privacy setting from the most restrictive or private setting to a less restrictive setting.

[206] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(2).

Control Visibility

Among the applications and services we evaluated, approximately 53% disclosed a qualitatively better response that users have control over how their personal information is displayed to others. However, our analysis indicates approximately 44% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 3% of applications and services evaluated discussed qualitatively worse practices that users do not have control over how their personal information is displayed to others.

It is imperative that children and students have agency and control over their personal information and user-generated content. This includes having the ability to determine privacy settings on the application or service for how their personal information is displayed to others; privately only to them, only with their patent or teacher, or with their friends, classmates, other classes, the entire school, or publicly to anyone on the Internet. However, there are still approximately 44% of applications and services that were unclear or indicated that users did not have control over how their personal information is displayed. It is likely that a large part of this percentage is the result of applications and services that do not have features to control whether information is private or public, and therefore do not disclose this practice in their policies, as described in the Visible Data section.

There is also likely some percentage of vendors who do not disclose this better practice in the policies, but still provide features or settings that give users control over how their information is displayed to others. Moreover, among applications and services that allow users to display information publicly, many vendors likely believe the inherent sharing purpose of the product to be self-evident, and therefore if children and students do not wish to make their information publicly available, they should not use the service. However, users may be unaware of the implications of applications' and services' usage of data and the necessary data collection required to use those applications and services, as such policies are an expected place to clarify this behavior prior to use. As a result, even though there is a very low percentage of policies that explicitly state they do not provide users with the ability to control how their information is displayed, an unclear response to this issue should be treated the same as a qualitatively worse response when making a decision whether or not to use an application or service.

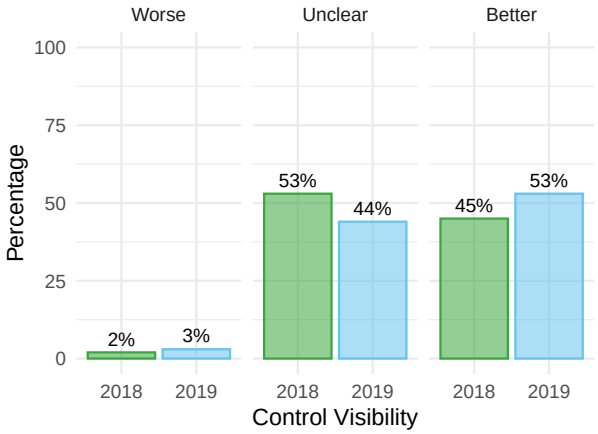


Figure 93: Do the policies clearly indicate whether or not a user has control over how their personal information is displayed to others?

Compared to 2018, applications and services evaluated in 2019 indicate an 8% increase in qualitatively better practices that companies disclose users have control over how their personal information is displayed to others. In addition, the majority of the 9% decrease in unclear practices shifted to qualitatively better disclosures from 2018 to 2019. From our analysis, 47% of applications and services, as seen in the Visible Data section, indicate a user's information can be displayed publicly which is lower than the approximately 53% qualitatively better response in the Control Visibility section. This positive trend is likely the result of over half the vendors updating their policies to indicate users have control over how their information is displayed. This practice, which can mitigate the risk associated with allowing children and students to make their personal information visible to others may also meet compliance obligations.[207]

Monitor Content

Among the applications or services we evaluated, approximately 29% disclosed a qualitatively better response that user uploaded content is reviewed, screened, or monitored by the vendor. However, our analysis indicates approximately 41% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 30% of applications and services evaluated discussed qualitatively worse practices that user uploaded content is not reviewed, screened, or monitored by the vendor.

Monitoring content is seen as a qualitatively better practice because these applications and services are intended for children and students, and monitoring content mitigates potential risks and harms by removing inappropriate materials and content related to bullying, alcohol, gambling, vio-

[207] *See* General Data Protection Regulation (GDPR), Data protection by design and by default, Art. 25(2).

lence, or pornography. From our informal observation, 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 only the content provided by the application or service, or user-created text based comments. Therefore, our findings that indicate approximately 41% are unclear on this question is not surprising because these vendors do not believe they need to disclose practices in their policies that they do not provide. However, approximately 30% of applications or services disclose they provide users the ability to upload and share content with others, but have no automatic or manual protections in place to review, screen, or monitor user-generated content. Applications and services that disclose they do not monitor any user-generated content may still allow users to upload content, and believe that content creators should bear primary responsibility for their speech and actions even though vendors state that they retain the ability to remove legal but objectionable content.[208]

However, allowing content creators to upload and share content with others, but not monitoring that content for inappropriate material, 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. As discussed in the Social Interactions section, applications and services intended for children and students should facilitate civil discourse and a safe environment by monitoring content shared with the service and prohibiting harassment, pornography, and other lawful but offensive or age-inappropriate material. If vendors do not have manual or automatic screening protections in place, children or students may be exposed to content that may cause social or emotional harm, 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.[209]

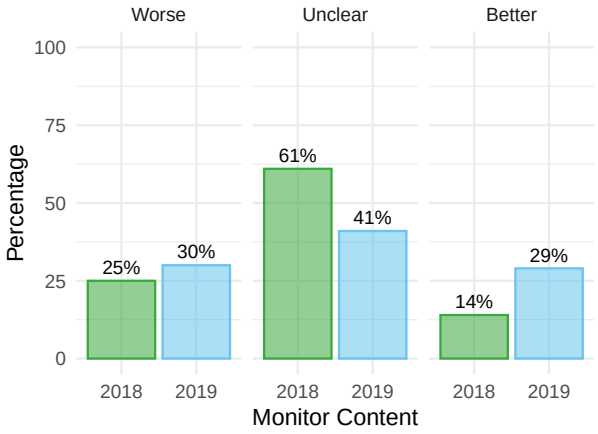


Figure 94: Do the policies clearly indicate whether or not the vendor reviews, screens, or monitors user-created content?

Compared to 2018, applications and services evaluated in 2019 indicate a 15% increase in qualitatively better practices that companies disclose user uploaded content is reviewed, screened, or monitored by the vendor. This positive trend may be the result of an increase in awareness on the part of teachers and parents wanting to help protect children from exposure to unwanted and inappropriate content. It may be that vendors updated their policies to disclose they engage in content monitoring as a positive safety factor when marketing their products to schools. Accordingly, this may be selection bias due to schools increasing their adoption of applications and services to help with their Children's Internet Protection Act (CIPA) compliance for e-rate purposes and for monitoring and tracking services of school-owned technology provided to students. However, even though since 2018 there has been a decrease of 20% in unclear practices, there is still a need for further transparency from vendors on this issue.

From our analysis, it appears there is approximately a 29% higher occurrence in the disclosure of qualitatively better practices, as compared to Filter Content. This is surprising given that monitoring content and filtering content for personal information are related practices. Lastly, with increased compliance issues and e-rate concerns always present for schools, it is recommended that vendors increase transparency and look at improving their practices of monitoring content used by children and students.

Filter Content

Among the applications and services we evaluated, approximately 15% disclosed a qualitatively better response that the vendor takes reasonable measures to delete all personal information from a user's postings before they are made publicly available. However, our analysis indicates approximately

208 The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230.
209 Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5)(B).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

59% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 26% of applications and services evaluated discussed qualitatively worse practices that the vendor does not take reasonable measures to delete all personal information from a user's postings before they are made publicly available.

It is especially important for vendors when dealing with personal information from children and students to provide protection from inadvertent disclosure of their personal information by filtering and deleting personal information from content or social interaction postings before they are visible to other children, students, or the public. Many applications and services do not collect any personal information and therefore are not required to obtain verifiable parental consent. However, the practice of filtering content or interactions by children and students can prevent the unintended collection of personal information and avoid the requirement to obtain parental consent, if the vendor takes reasonable measures to delete all personal information from a child's postings before they are made public, and also to delete the information from its records.[210] However, almost twice as many policies disclose qualitative worse practices in this regard and approximately 59% are unclear in this respect.

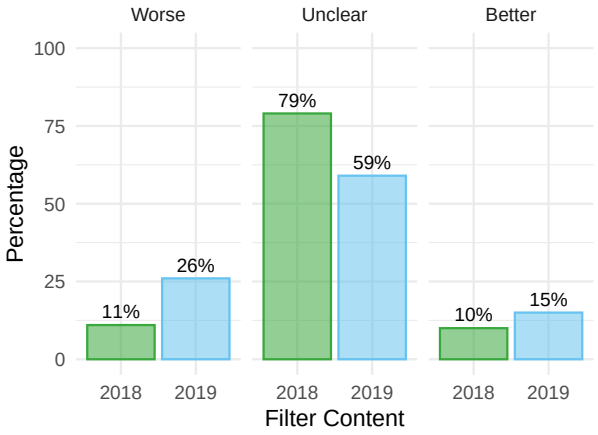


Figure 95: Do the policies clearly indicate whether or not the vendor takes reasonable measures to delete all personal information from a user's postings before they are made publicly visible?

Compared to 2018, applications and services evaluated in 2019 indicate a 5% increase in qualitatively better practices that companies disclose they take reasonable measures to delete all personal information from a user's postings before they are made publicly available. In addition, since 2018 there has been a 20% decrease in unclear practices and a respective 15% increase in qualitative worse practices of vendors disclosing they do not delete personal information from a user's postings before they are made publicly available. Compared to the Visible Data section, it appears that approximately 47% of policies disclose that child or student information can be made publicly visible, but only 15% of policies indicated that the vendor takes reasonable measures to filter and delete personal information before posting. This roughly 30% lower occurrence of better practices to filter content may be because vendors who disclose information can be made public also disclose the ability for users to control their visibility with privacy settings, as discussed in the Control Visibility section. In addition, the majority of vendors likely cannot avoid the collection of personal information due to the nature of their application and service and therefore already obtain verifiable parental consent, as discussed in the Parental Consent section, which indicates they do not need to take advantage of the compliance exception for filtering content of personal information and may continue to remain unclear on this issue.

However, even though the percentage of unclear practices decreased approximately 20% since 2018, the percentage of vendors with unclear practices of both the Monitor Content and Filter Content sections is still too high. When these practices are not 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.

Moderating Interactions

Among the applications or services we evaluated, approximately 15% disclosed a qualitatively better response that interactions between users of the application or service are moderated. However, our analysis indicates approximately 65% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 20% of applications and services evaluated discussed qualitatively worse practices that interactions between users of the application or service are not moderated.

This disclosure of qualitatively better responses is significantly lower than expected, given the practice of moderating safe and unsafe interactions of children or students mitigates the practices disclosed by 61% and 42% of applications and services that allow for safe and unsafe interactions respectively, as described in the Safe Interactions and Unsafe Interactions sections. In addition, the approximately 20% that disclose qualitatively worse responses that they do not moderate social interactions between users is likely related to those vendors that disclose their application and services are not intended for children or students and therefore claim they are not required to moderate interactions for compliance purposes, as discussed in Intended Users sec-

[210] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

tion. However, 65% of applications and services evaluated were unclear on this issue; this may be because they do not provide social interaction features, or if these features are available, it is not evident to vendors that this is a compliance obligation and should be disclosed in their policies. Additionally, parents and educators use this detail as a differentiating factor when making an informed decision to use the product. It is recommended that applications and services that provide social interaction features 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 and after they are made publicly available to children, students, or others. These protections are intended to prevent potential social and emotional harm as a result of harassment, stalking, and/or cyberbullying using these communication platforms.[211]

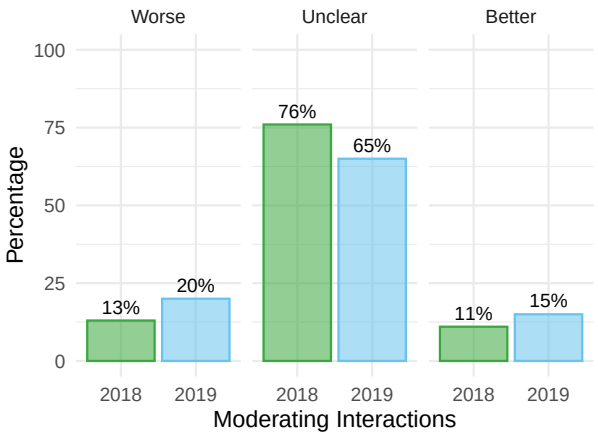


Figure 96: Do the policies clearly indicate whether or not social interactions between users of the product are moderated?

Compared to 2018, applications and services evaluated in 2019 indicate a 4% increase in qualitatively better practices that companies disclose interactions between users of the application or service are moderated. In addition, there was also a corresponding decrease of 11% in unclear responses. This positive trend of transparency may be the result of increased awareness of the privacy risks and harms of interactions between children students with trusted and untrusted individuals and the increasing concerns that schools and parents raise around this issue. However, there was also a 7% increase in qualitatively worse practices that interactions between users of the application or service are not moderated. As discussed in the School Contract section, the lack of more prevalent moderation is likely the result of companies that enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent moderating of social interactions between students. These companies may assume that because the contract discloses the school or district faculty control of the deployment of the application or service and administration of student accounts that they do not also need to disclose moderating practices in their policies.

From our analysis, it appears there is roughly the same percentage of qualitatively better practices for this issue, as compared to Log Interactions. However, it appears that there is a 19% higher incidence of qualitatively worse practices of not moderating interactions as compared to not logging interactions. This likely further supports our analysis that companies that enter into contracts with schools and districts require the school or district to control any moderating process, but remain unclear on whether or not those interactions are logged. Depending on the deployment of the application or service these actions could be performed by the vendor or the school, or both. It is recommended that vendors increase their transparency on whether or not they moderate interactions and, where appropriate, disclose whether a school or district is responsible for moderating interactions to provide future expectations and trust on behalf of parents, teachers, schools, or districts about how collected information from children and students will be moderated in order to meet their expectations of privacy.

Log Interactions

Among the applications and services we evaluated, approximately 14% disclosed a qualitatively better response that social interactions are logged by the vendor. However, our analysis indicates approximately 85% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 1% of applications and services evaluated discussed qualitatively worse practices that social interactions are not logged by the vendor.

Schools have varying degrees of capabilities to effectively log interactions between users on applications and services used in the classroom, but most schools have found that a documenting student and educator social interactions leads to an easier resolution of potential conflict in this increasingly technology based school environment. However, logging of students' personal information, usage information, and behavioral information through the use of email, chat communications, and use of the product itself can increase the risk that the information may be used or disclosed in unintended ways, as discussed in the Collect PII, Usage Data, or Behavioral Data sections. Further, school officials have also discovered that when students are aware that their interactions with the applications and services used at school are monitored, or that the capability for surveillance of some kind

[211] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

exists, it affects their behavior and learning outcomes.[212] In some cases, logging can provide important details for student assessment, education record management, or even disciplinary or legal action. As discussed in the School Contract section, this large percentage of unclear practices is likely the result of companies that enter into contracts with schools and districts and require the school or district to control the collection of personal information and logging all interactions of students. However, the large percentage of unclear practices may be the result of applications or services that do not have the capability for logging interactions, but vendors should still increase their transparency on this important practice. In our evaluation process, it is a better practice to disclose whether or not logging can occur and if it is controlled by the vendor who has access to those logs, as discussed in the Employee Access section.

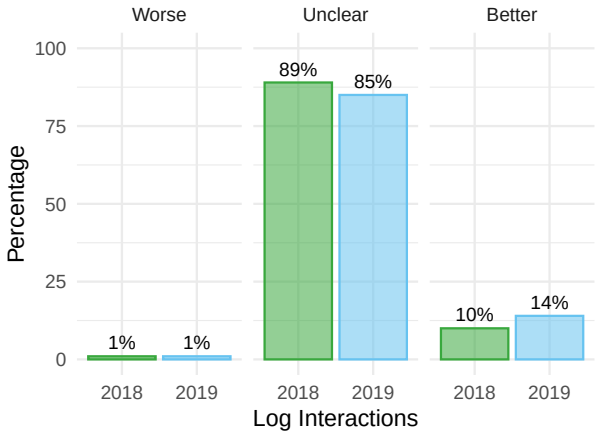


Figure 97: Do the policies clearly indicate whether or not social interactions are logged by the vendor and available for review or audit?

Compared to 2018, applications and services evaluated in 2019 indicate a 4% increase in qualitatively better practices that companies disclose social interactions are logged by the vendor. However, qualitatively worse practices have remained approximately unchanged over the same time period and unclear practices have decreased by 4%. This slightly positive trend may be the result of increased concern in educational settings about surveillance technologies that capture student interactions in applications or services used in the classroom, and requiring vendors to disclose whether logging features are part of the safety features of the product.

From our analysis, it appears there is an approximately 47% lower occurrence in the disclosure of qualitatively better practices for this issue, and a 49% higher occurrence of unclear responses, as compared to Safe Interactions. This may suggest that the majority of applications and services that provide safe interactions do not log interactions, or there are private agreements in place between the school or district with the vendor to control logging features. While this might not be appropriate in every situation, it is certainly worth noting the large gap between these two categories. It is recommended that vendors take a closer look at any interaction features they provide–both safe and unsafe–and whether or not interactions are provided, vendors should be transparent in their policies on what information is logged, how that information is accessed, retained, and/or made available.

Report Abuse

Among the applications and services we evaluated, approximately 14% disclosed a qualitatively better response that a user can report abusive behavior or cyberbullying. However, our analysis indicates approximately 84% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 2% of applications and services evaluated discussed qualitatively worse practices that a user cannot report abusive behavior or cyberbullying.

The ability to report abuse and cyberbullying is becoming increasingly important to teachers and parents to protect children who are spending more time online both in-and-out of school, as discussed in the Social interactions section. While most schools have a system-wide mechanism for reporting abusive behavior for compliance purposes, it is helpful to have a check and balance system inside of each application or service that children and students use at home or in the classroom.[213] Allowing abusive behavior to be reported closer to the source can allow for more context to be captured or attached to the incident which may be helpful in appropriately resolving situations. The high percentage of unclear responses may be due to applications and services that lack the capability or features to report abuse to the vendor, or their parent or educator. However, as compared to the Safe interactions section, our analysis indicated 61% disclosed a transparent response that users can interact with trusted users, but only 14% indicated they provide users the ability to report abusive behavior or cyberbullying. This reporting functionality helps to create a safe environment for children and students to interact.

[212] Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). Privacy risks and harms, San Francisco, CA: Common Sense Media.

[213] *See* Cal. Penal Code § 653.2; Cal. Educ. Code §§ 32261, 48900, 66302.

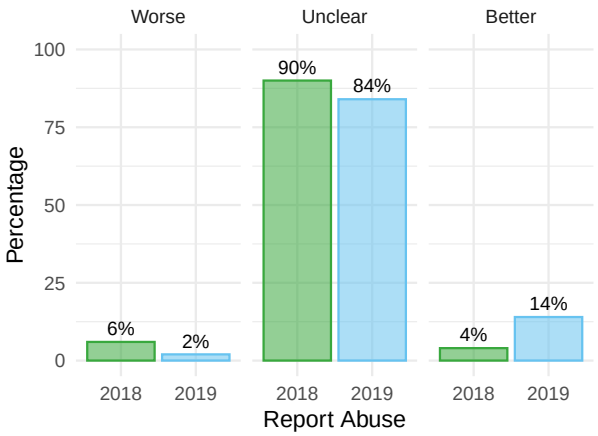


Figure 98: Do the policies clearly indicate whether or not a user can report abusive behavior or cyberbullying?

Compared to 2018, applications and services evaluated in 2019 indicate a 10% increase in qualitatively better practices that a user can report abusive behavior or cyberbullying. There is also a 4% decrease in qualitatively worse practices that a user cannot report abusive behavior or cyberbullying. This positive trend is likely the result of an increased awareness of digital-wellbeing initiatives and focus on the social, emotional, and physical harm that can result from cyberbullying and harassment online. From our analysis, it appears there is approximately a 47% lower occurrence in the disclosure of qualitatively better practices for this issue, as compared to Safe Interactions, along with a 28% lower occurrence compared to the qualitatively worse practice of allowing Unsafe Interactions. This would seem to indicate that vendors are disclosing interactions, both safe and unsafe, but not providing a means to report abuse and cyberbullying within the application or service.

This may be the result of vendors including other means of safeguarding children beyond reporting abuse, such as limiting interactions to only other students in the same classroom, or only interacting with other friends that a child knows with parental supervision. However, our evaluation process recommends vendors increase their transparency on this important issue and disclose whether users have the ability to report any abusive interactions with other users in order to block those interactions, but also to prevent abuse or harassment from happening to other children or students. These features also serve to fill the gap between safe and unsafe interactions when parent or educator supervision is not available and provide parents and educators with more information about the safety features of the application or service to meet their expectations of privacy.

Full: Ads and Tracking

The concern of Ads & Tracking primarily examines practices where children's or students' information is used for first- or third-party marketing purposes, third-party tracking, to display behavioral or contextual advertisements, for the creation of data profiles and they have the ability to unsubscribe.

Traditional advertisements (otherwise referred to as contextual advertisements), display products and services to users based only on the relevant content or webpage in which the user is currently viewing, but contextual ads do not collect any specific information about the user in order to display these ads. 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 to a more specific targeted audience that may be more directed to users 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 often use these services with a lower expectation of privacy, but our analysis observed both free and paid services' policies discussed displaying advertisements. However, we informally observed among the applications and services evaluated that required parent, teacher, or district paid subscriptions, or student in-App-Purchases, the majority did not disclose they 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 or subscription edtech services that often require the school or district to enter into a contract or student data privacy agreement which prohibits advertising practices with students. 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.

Ads and Tracking Scores

Figure 99 illustrates the Ads & Tracking scores among all applications and services evaluated. Table 21 compares and summarizes the Ads & Tracking concern score minimum,

maximum, median, mean, Q1 (point between the 1st and 2nd quartile), and Q3 (point between the 3rd and 4th quartile).

Table 21: 2018 vs. 2019 Ads & Tracking score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	0	20	40	38	56	85
2019	0	35	55	50	65	95

From the analysis of 10 related questions in the concern, we determined a median in 2019 of approximately 55%. This median is lower than expected, given these applications and services are intended for children and students and a majority of companies disclose qualitatively better practices that they limit the collection of personal information from children.

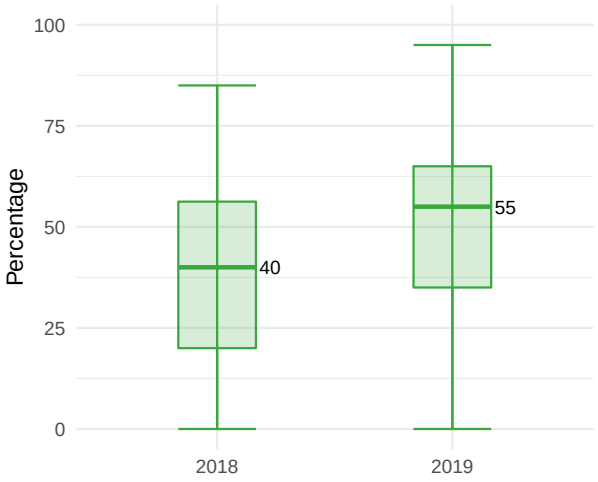


Figure 99: Comparison of Ads & Tracking scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of Ads & Tracking indicate a 37% increase in median scores that indicate more transparent and qualitatively better practices of collecting personal information. In addition, since 2018 the industry has consolidated and increased the range of scores, and significantly improved its practices regarding Ads & Tracking as seen by the 2019 median of 55% equalling Q3 from 2018 for the concern of Ads & Tracking. This positive trend is not surprising as our Evaluation Tiers primarily focus on improving advertising and tracking related practices of applications and services used by children and students.

Third-Party Marketing

Among the applications and services we evaluated, approximately 47% disclosed a qualitatively better response that collected personal and non-personal information is never used for any third-party marketing purposes. However, our analysis indicates approximately 21% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 32% of applications and services evaluated discussed qualitatively worse practice that collected personal and non-personal information is used for third-party marketing purposes.

Accordingly, 21% of applications and services with unclear practices is likely because many do not display any marketing related first or third-party advertisements. Therefore, these applications and services believe it to be self-evident that if no marketing advertisements are displayed, then a user's data would not be used for any unsolicited marketing purposes. However, when marketing practices are not 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.

From a parent or teacher's perspective, there is not any meaningful distinction between the display of advertisements and the use of children or student's information for marketing communications. First-party marketing communications are from the application or service that the child or student already has a relationship with and is considered a different practice in our evaluation. Moreover, first-party marketing communicates additional products and features from a company that children, students, parents, and educators are already familiar with. In contrast, third-party marketing communications are from an application or service that a child or student does not have a direct relationship with and therefore is a different practice because it communicates unrelated or unsolicited products and features from third-party companies. Surprisingly, a large percentage of applications and services disclose they use child or student personal information for advertising or marketing purposes. Given these products are intended for children and students, they may be in violation of federal or state law if other protections are not put in place to exclude data from children and students if the application or service is intended for a mixed audience.[214,215,216]

[214] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2

[215] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).

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

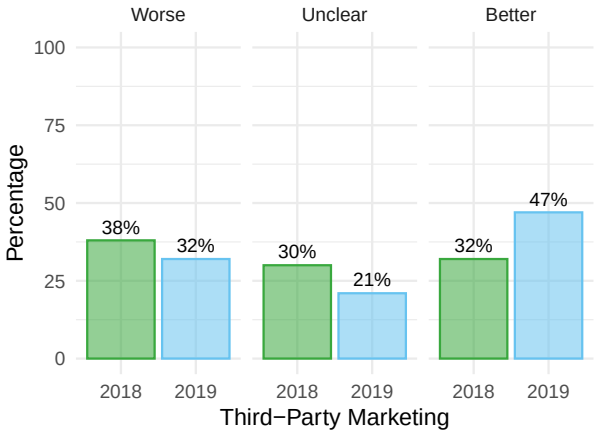


Figure 100: Do the policies clearly indicate whether or not personal information is shared with third parties for advertising or marketing purposes?

Compared to 2018, applications and services evaluated in 2019 indicate a 15% increase in qualitatively better practices that collected personal information is never used for third-party advertising or marketing purposes. In addition, since 2018 our findings indicate a positive trend with a 6% decrease in qualitatively worse practices and 10% decrease in unclear practices. This positive trend is not surprising as our Evaluation Tiers focus on improving third-party marketing related practices of applications and services used by children and students. Additionally, among the applications and services collecting child or student personal information for advertising or marketing purposes, many companies often 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 analyses how vendors respect the different context between acceptable and unacceptable use of collected information for marketing purposes. For example, when personal information is collected and used from parents and teachers for explicit marketing purposes, that is a different context than when personal information is collected for a separate and compliance related context of providing parental consent for their child or student's use of the service. Moreover, a combined 52% of applications and services are either unclear or disclose they engage 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 that engage in third-party marketing using personal information, 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.

Traditional Ads

Among the applications and services we evaluated, approximately 23% disclosed a qualitatively better response that they do not display any traditional or contextual advertisements to children or students. However, our analysis indicates approximately 30% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 47% of applications and services evaluated discussed qualitatively worse practices that they display any traditional advertisements to children or students.

Applications and services that disclosed they may display traditional advertisements to users likely do so 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. Through an informal observation, we determined among applications and services that clearly displayed traditional advertisements, many did not disclose advertising practices in their policies. This behavior may be because these applications and services believed the practice of displaying advertisements to be self-evident and they did not need to disclose that practice in their policies. Moreover, among applications and services that were unclear but did not display any advertisements, it is assumed their lack of transparency is because they do not believe they need to disclose practices they do not engage in. However, when these practices are not disclosed, there is no future expectation or trust on behalf of parents, teachers, schools, or districts about whether or not advertising will be displayed to children and students in order to meet their expectations of privacy.

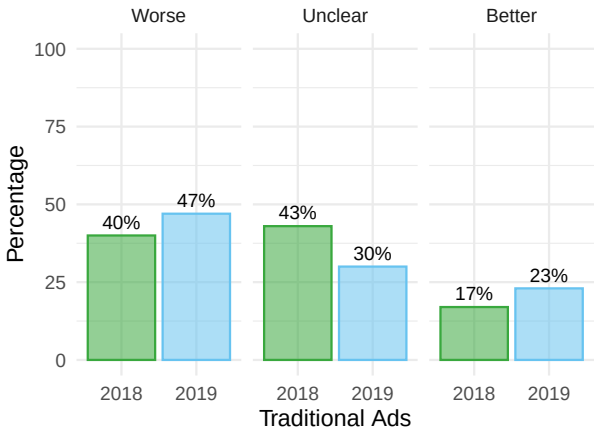


Figure 101: Do the policies clearly indicate whether or not traditional advertisements are displayed to a user based on a webpage's content, and not that user's data?

Compared to 2018, applications and services evaluated in 2019 indicate a 6% increase in qualitatively better practices that they do not display any traditional or contextual advertisements to children or students. In addition, since 2018 our findings indicate a positive trend with a 13% decrease in unclear practices, but 6% increase in qualitatively worse practices. This positive trend of companies updating their unclear practices with qualitatively better practices is not surprising as our Evaluation Tiers focus on improving advertising related practices of applications and services used by children and students.

Compared to our analysis in the Behavioral Ads section, approximately 9% more applications and services appear to be unclear in their policies about contextual ads than behavioral ads. Additionally we see an approximate 14% higher incidence of displaying Traditional Ads (47%) versus Behavioral Ads (33%) However, this discrepancy is expected, as compliance obligations for applications and services intended for children provide an exception for companies to display contextual advertising that does not use any personal information, which excludes behavioral advertising.[217] Lastly, the percentage of unclear practices on this issue, as compared to the Behavioral Ads section, should also take into account conflicting Federal and State laws that provide an important distinction between contextual advertising directed to students.[218]

Behavioral Ads

Among the applications and services we evaluated, approximately 46% disclosed a qualitatively better response that collected information is never used for any behavioral advertising. However, our analysis indicates approximately 21% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 33% of applications and services evaluated discussed qualitatively worse practices that collected information is used to display behavioral advertising.

From our previous analysis of personal information used for marketing purposes in the Third-Party Marketing section, our findings indicate a similar amount (46%) of applications or services disclosed that no personal information is used for advertising or marketing purposes. In addition, it appears that because the use of collected information for behavioral advertising or third-party marketing poses the same compliance risk from the perspective of vendors, our findings indicate a similar amount (32%) of applications or services disclosed qualitatively worse findings. Moreover, our findings indicate a similar percentage of companies remain unclear on behavioral advertising and third-party marketing, likely because those applications and services do not engage in those practices. It may be that among the applications and services that are unclear on this issue, many provide contextual advertising, but believe it is confusing to explain the compliance related distinction between their use of contextual advertising in one instance, and behavioral advertising in another instance.

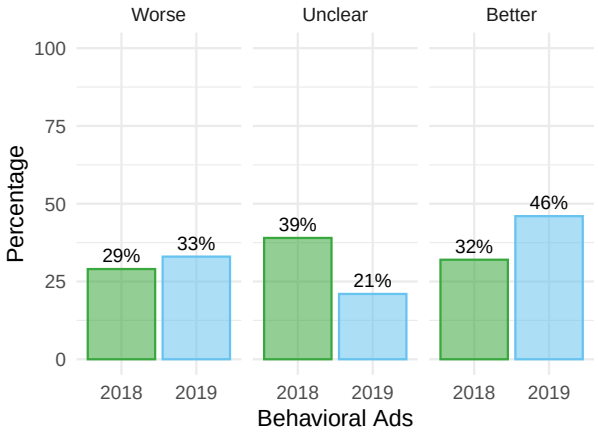


Figure 102: Do the policies clearly indicate whether or not behavioral advertising based on a user's personal information are displayed?

Compared to 2018, applications and services evaluated in 2019 indicate a 14% increase in qualitatively better practices that collected information is never used for any behavioral advertising. In addition, since 2018 our findings indicate a positive trend with an 18% decrease in unclear practices, but 3% increase in qualitatively worse practices. This positive trend of companies updating their unclear practices with qualitatively better practices is not surprising as our Evaluation Tiers focus on improving behavioral advertising related practices of applications and services used by children and students.

Accordingly, this shift since 2018 from unclear practices to qualitatively worse disclosures on such an important compliance related issue for children and students, is likely because many applications and services disclose their behavioral advertising practices are only targeted to parents and educators and not children or students in order to avoid potential violations of federal or state law.[219,220,221,222] Similarly with the Third-Party Marketing section, among the 32% of applications and services with qualitatively worse practices, many use language to restrict their use to only parent or

217 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

218 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).

219 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

220 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).

221 California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(9).

222 *See* General Data Protection Regulation (GDPR), Art. 3(2)(a)-(b), 4(11).

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 are intended for children and students who are generating the majority of interaction data. From our evaluation process we observed many applications and services that provide secondary "Parent" or "Teacher" accounts or related applications or services to monitor their 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 teachers 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. In addition, anonymized or deidentified behavioral data from a child or student's use of the application or service could be associated with a teacher or parent account. This associated data could then be used to circumvent intended protections either through recombination or re-identification of the data with third parties, or to display behavioral ads to the parent or teacher.

Third-Party Tracking

Among the applications and services we evaluated, approximately 35% disclosed a qualitatively better response that collected information will never be used by third-party advertising or tracking technologies. However, our analysis indicates approximately 24% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 41% of applications and services evaluated discussed qualitatively worse practices that collected information is 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 opaque processes, or for marketing or advertising purposes.[223,224,225] From our analysis, it appears there is approximately an 11% lower occurrence in the disclosure of qualitatively better practices for this issue, as compared to the Behavioral Ads section, but a relative increase in qualitatively worse practices of approximately 8%. It appears that most applications and services shift their qualitatively better practices about behavioral advertising to qualitatively worse practices for third-party tracking. This shift of companies updating their unclear practices to disclose both qualitatively better and worse practices of third-party tracking is surprising. We would have expected industry to shift from unclear to qualitatively better practices given the increased attention on this important issue. However, these findings reflect what we would expect based on observation where we see a dramatic increase in desktop and mobile third-party advertising trackers used in mainstream web applications and services in recent years.[226,227] The Privacy Program is also actively researching this issue area, and a report expected in Q4 2019, will provide more insight into advertising and tracking behavior. Therefore, we would expect more policies to include better transparency 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.

However, unlike other marketing or advertising indicators, it appears vendors are neither aware nor believe that there is currently a comparative advantage to disclosing they do not engage in the qualitatively worse practice of third-party tracking. This is also likely the result of no legislation covering tracking practices and the practice being largely invisible to end users. Given that approximately 24% of applications and services are unclear on this issue, it is recommended that companies change their policies in order to provide notice to consumers about whether or not their product uses third-party advertising or trackers; third-party tracking practices are ultimately no different than other methods of collecting behavioral information for marketing or advertising purposes.

223 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

224 California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(7).

225 California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.140(o)(1)(A), (x).

226 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.

227 Fouad, Imane & Bielova, Nataliia & Legout, Arnaud & Sarafijanovic-Djukic, Natasa, *Tracking the Pixels: Detecting Unknown Web Trackers via Analysing Invisible Pixels*, (2019), https://arxiv.org/pdf/1812.01514.pdf.

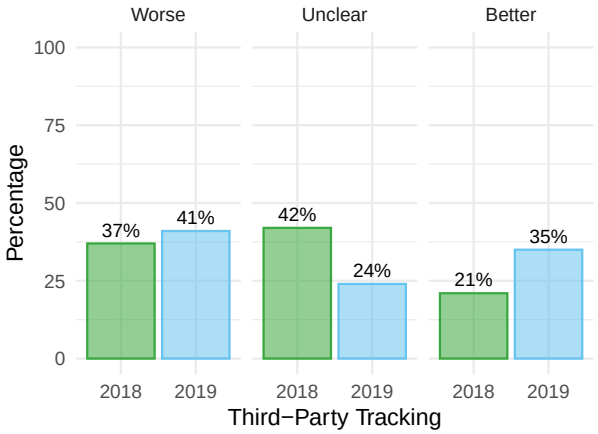


Figure 103: Do the policies clearly indicate whether or not third-party advertising services or tracking technologies collect any information from a user of the product?

Compared to 2018, applications and services evaluated in 2019 indicate a 14% increase in qualitatively better practices that collected information will never be used by third-party advertising or tracking technologies. In addition, since 2018 our findings indicate a positive trend with an 18% decrease in unclear practices, but some of those gains went to a 3% increase in qualitatively worse practices. This positive trend of companies updating their unclear practices with qualitatively better practices is not surprising as our Evaluation Tiers focus on improving third-party tracking related practices of applications and services used by children and students. Therefore, our findings indicate companies are likely updating their practices and policies to move away from directly monetizing users' personal information with third-party marketing or behavioral advertising on their applications or services. Instead our findings indicate companies in 2019 are moving towards integrating with third-party advertising tracking networks that display advertisements to users on devices and applications and services other than the company's product itself, as described in the Track Users section.

Track Users

Among the applications and services we evaluated, approximately 38% 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. However, our analysis indicates approximately 29% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 33% of applications and services evaluated discussed qualitatively worse practices that collected information is 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 opaque processes, or for marketing or advertising purposes. From our analysis, it appears there is approximately an 8% 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 applications services across the Internet.

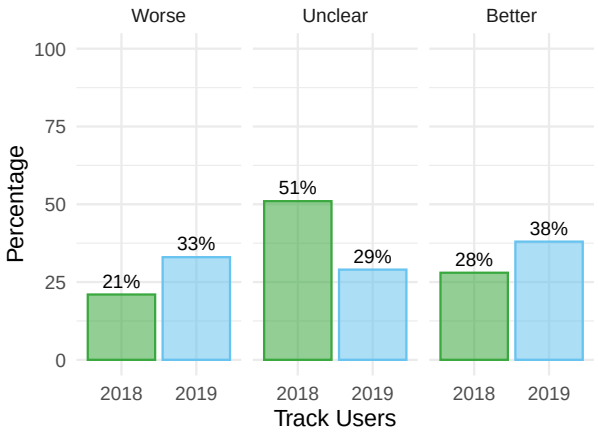


Figure 104: Do the policies clearly indicate whether or not a user's information is used to track users and display target advertisements on other third-party websites or services?

Compared to 2018, applications and services evaluated in 2019 indicate a 10% increase in qualitatively better practices that collected information will never be used to track and target advertisements to users on other third-party websites or services. In addition, since 2018 our findings indicate a positive trend with a 22% decrease in unclear practices, but some of those gains went to an 12% increase in qualitatively worse practices. This positive trend of companies updating their unclear practices with qualitatively better practices is not surprising as our Evaluation Tiers focus on improving tracking related practices of applications and services used by children and students.

Among the 32% of applications and services with qualitatively worse practices, a majority of policies use language to try and restrict their use of tracking to only parent or teacher

information in order to avoid compliance issues with children or students, as discussed in the Intended Users section. However, this distinction is difficult to apply in practice and may not adequately exculpate vendors from potential compliance violations of tracking children or students even if done so inadvertently.[228,229,230,231,232] Moreover, the relative percent increase in unclear and qualitatively better practices, as compared to the Third-Party Tracking section, may be the result of 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. Therefore, our findings indicate companies may be updating their policies to move away from directly monetizing users' personal information with third-party marketing or behavioral advertising on their applications or services. Instead our findings indicate companies in 2019 are moving towards using third-party advertising tracking networks to indirectly display advertisements to users on other devices and applications and services those users may use across the Internet and over time rather than on the company's product itself.

Data Profile

Among the applications and services we evaluated, approximately 44% disclosed a qualitatively better response that collected information will not be used by the company to create an advertising profile, engage in data enhancement, or target advertising. However, our analysis indicates approximately 33% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 23% of applications and services evaluated discussed qualitatively worse practices that collected information is used by the company 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 considered another indirect method in 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.[233,234,235,236] As compared with other marketing or advertising indicators in the Ads & Tracking concern, this issue has the highest relative percentage of unclear practices and lowest percentage of qualitatively worse disclosures. Simply stated: the majority of applications and services evaluated have unclear and worse practices. Perhaps this is due to a lack of parent and educator awareness regarding the importance of this issue. Or perhaps this is due to the lack of enforcement of legislation related to creating advertising profiles of students.

Among the approximately 33% with unclear practices, it appears many vendors still do not make the distinction between using personal information for advertising or marketing purposes and using non-personal information for amassing a profile or sharing 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 71% of applications and services disclose qualitatively better practices that they place contractual limitations on third parties, as discussed in the Third-Party Limits section, which, depending on the terms of those limits, can mitigate otherwise unclear responses to whether collected information can be used to create an advertising profile.[237,238]

228 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

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

230 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(B).

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

232 California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.140(o)(1)(A), (x).

233 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

234 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(2), 22584(e)(2).

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

236 California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(o)(1)(K).

237 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.

238 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(i)-(ii).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

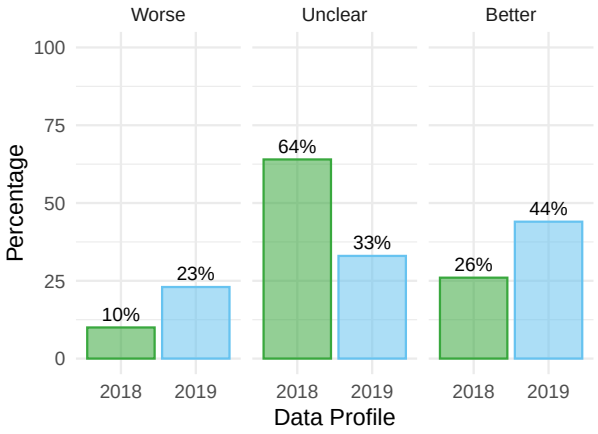


Figure 105: Do the policies clearly indicate whether or not the vendor allows third parties to use a student's data to create an automated profile, engage in data enhancement, conduct social advertising, or target advertising to students, parents, teachers, or the school?

Compared to 2018, applications and services evaluated in 2019 indicate an 18% increase in qualitatively better practices that student's data will not be used by the third parties to create an advertising profile, engage in data enhancement, or target advertising to students, parents, teachers, or the school. In addition, since 2018 our findings indicate a positive trend with a 31% decrease in unclear practices, but some of those gains went to a 12% increase in qualitatively worse practices. This is the most significant positive trend in the Ads & Tracking concern of companies updating their unclear practices with qualitatively better practices that collected information will not be used to create an advertising profile. This positive trend is likely the result of companies updating their policies for compliance purposes to incorporate new privacy rights granted by changing International and U.S., state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018 and provided many new privacy rights for companies subject to the GDPR's requirements including disclosing the existence of automated decision-making, including profiling.[239,240] This positive trend is also not surprising as our Evaluation Tiers focus on improving data profiling related practices of applications and services used by children and students.

For those companies with unclear policies, the existence of automated decision-making, including profiling children or students for advertising purposes, may be confused as the same as Behavioral Ads or Third-Party Tracking. However, vendors should be aware that amassing a profile of a child or student for non-K-12 educational purposes is a prohibited broader use of collected information, because the amount and type of collected data goes beyond the scope of behavioral information.[241] Therefore, parents and teachers need to exercise caution when evaluating whether to use popular edtech applications and services that allow advertising profiles to be amassed, and vendors need to provide greater transparency on this issue. When these practices are not 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.

Marketing Messages

Among the applications and services we evaluated, approximately 4% disclosed a qualitatively better response that the company does not send first-party marketing emails, text messages, or other related communications to its users. However, our analysis indicates approximately 25% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 71% of applications and services evaluated discussed qualitatively worse practices that the company does send first-party marketing emails, text messages, or other related communications that may be of interest to its users.

Accordingly, applications and services with unclear practices is likely because many do not send any marketing related communications. Therefore, these applications and services may believe it to be self-evident that if no marketing communications are sent to its users, then they would not need to disclose practices they do not engage in. However, when marketing practices are not 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. First-party marketing communications are distinct from Third-Party Marketing communications for our evaluation purposes. First-party marketing communications are from the application or service that the child or student already has a relationship and account with. These marketing messages communicate additional products and features from a company that children, students, parents, and educators are already familiar with. Surprisingly, a large percentage of applications and services disclose they use child or student personal information for first-party marketing purposes.

239 *See* General Data Protection Regulation (GDPR), Art. 4(4), 13(2)(f), 14(2)(g), 15(1)(h), 22(1)-(3).

240 *See* General Data Protection Regulation (GDPR), Art. 28(2)-(4), 29.

241 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(2).

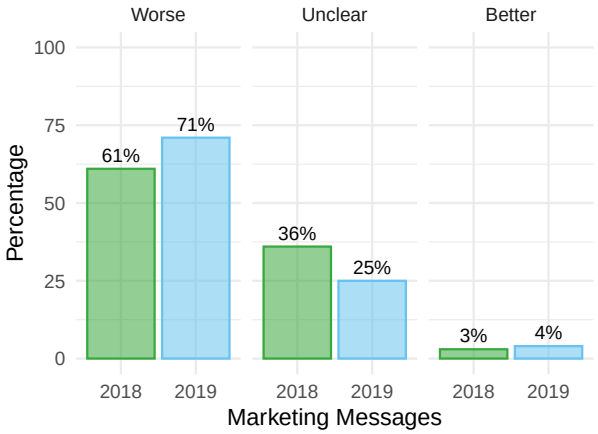


Figure 106: Do the policies clearly indicate whether or not the vendor may send marketing emails, text messages, or other related communications that may be of interest to a user?

Compared to 2018, applications and services evaluated in 2019 indicate a marginal 1% increase in qualitatively better practices that the company does not send first-party marketing emails, text messages, or other related communications to its users. In addition, since 2018 our findings indicate a negative trend with an 11% decrease in unclear practices, but 10% increase in qualitatively worse practices. This negative trend may be the result of companies updating their unclear practices to clarify that they engage in first-party marketing to children and students which is not prohibited.[242,243,244]

Third-Party Promotions

Among the applications and services we evaluated, approximately 1% disclosed a qualitatively better response that the company does not provide users the opportunity to participate in any sweepstakes, contests, surveys, or other similar promotions. However, our analysis indicates approximately 58% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 41% of applications and services evaluated discussed qualitatively worse practices that the company does not ask users to participate in any sweepstakes, contests, surveys, or other similar promotions.

Accordingly, providing users the opportunity to participate in sweepstakes, contests, or surveys is considered qualitatively worse in our evaluation process because a company should not request, prompt, entice, or encourage children or students to provide personal information with the use of prizes or games.[245] Similarly, as discussed in the Collection Limitation section data collection should be limited to data necessary for using the product. In addition, this practice can involve data collection of children and students by third-party companies in ways beyond the context of the application or service. For example, third parties can provide sweepstakes, contests, or a survey themselves on behalf of the first-party company, or simply provide the prize or incentive directly to the winner based on a data-sharing agreement with the application or service.

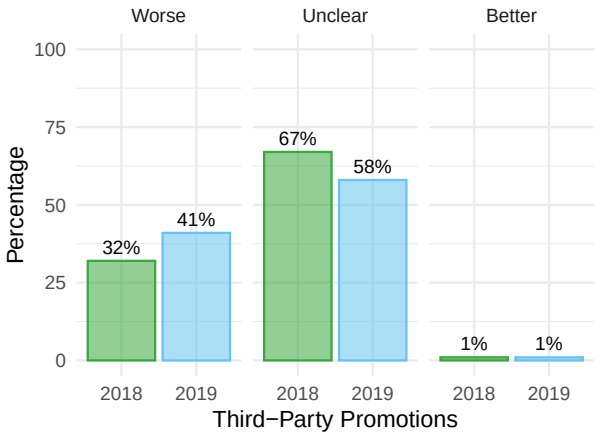


Figure 107: Do the policies clearly indicate whether or not the vendor may ask a user to participate in any sweepstakes, contests, surveys, or other similar promotions?

Compared to 2018, applications and services evaluated in 2019 indicate no change in qualitatively better practices that the company does not provide users the opportunity to participate in any sweepstakes, contests, surveys, or other similar promotions. Similarly to our findings in the Marketing Messages section, since 2018 our findings indicate a negative trend with a 9% increase in qualitatively worse practices. This negative trend is likely the result of companies clarifying they provide third-party sweepstakes, contests, surveys, or other similar promotions to children and students which are optional and not required to be completed to use the application or service, and are not provided by the vendor to collect more personal information, and therefore not prohibited under the law, but this is still considered a worse practice depending on the content of the promotion and the nature of its educational purpose.[246,247] Moreover, third-party providers or affiliates of the vendor may send promo-

242 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.7.

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

244 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).

245 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(d).

246 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.7.

247 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).

tional communications to children and students in order to collect personal information, which is not considered third-party marketing because there is no product offered for purchase and participants do not need to pay to win. These promotions provide the opportunity for a child, student, or their parent or educator to win a prize through the submission of personal information to enter the contest, survey or sweepstakes. Parents and educators should use caution when providing their personal information to third party companies for promotional purposes or providing consent for children and students to participate which could put them at a greater risk for exploitation, identity theft, and misuse of their data for marketing or advertising purposes.

Unsubscribe Ads

Among the applications and services we evaluated, approximately 37% disclosed a qualitatively better response that users can unsubscribe or opt out from traditional or behavioral advertising. However, our analysis indicates approximately 59% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 4% of applications and services evaluated discussed qualitatively worse practices that users cannot unsubscribe or opt out from traditional or behavioral advertising.

Among applications and services with unclear practices, it is assumed their lack of transparency is because they do not disclose opt-out functionality related to advertisements they do not display. As compared to the Traditional Ads and Behavioral Ads section, approximately 47% and 33% respectively disclose they display contextual or behavioral advertisements, but 37% disclose they allow users to provide opt-out consent from traditional or behavioral advertising. It appears the percentage of products that provide the ability to opt out from advertising is higher than the percent that display behavioral advertisements, but lower than the percent that display traditional advertisements. This might mean the use of collected information for behavioral advertising poses a unique compliance risk from the perspective of vendors, and those applications and services are more likely to provide an opportunity to provide opt-out consent than for products with only traditional advertising.[248,249] However, when these practices are not 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.

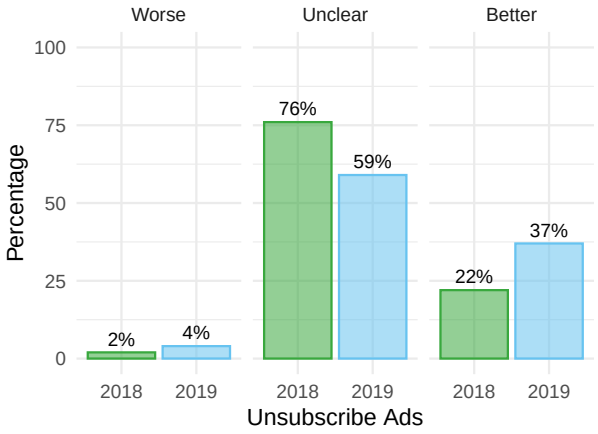


Figure 108: Do the policies clearly indicate whether or not a user can opt out of traditional or behavioral advertising?

Compared to 2018, applications and services evaluated in 2019 indicate a 15% increase in qualitatively better practices that users can unsubscribe from traditional or behavioral advertising. In addition, since 2018 our findings indicate a positive trend with a 17% decrease in unclear practices, and only 2% increase in qualitatively worse practices. This positive trend is likely the result of companies clarifying their existing practices that they allow users to unsubscribe from traditional or behavioral advertising.

Unsubscribe Marketing

Among the applications and services we evaluated, approximately 67% disclosed a qualitatively better response that users can unsubscribe or opt out from first- or third-party marketing communications. However, our analysis indicates approximately 32% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 1% of applications and services evaluated discussed qualitatively worse practices that users cannot unsubscribe or opt out from first- or third-party marketing communications.

Among applications and services with unclear practices, it is assumed their lack of transparency is because they do not believe they need to disclose functionality related to unsubscribing or opting-out from advertisements they do not display. As compared to the Marketing Messages and Third-Party Marketing sections, approximately 71% and 32% respectively provide first-party marketing messages, or third-party marketing communications, but 67% disclose they allow users to unsubscribe or opt out from marketing communications. As discussed in the Third-Party Marketing section, this may mean the use of collected information for third-party marketing poses a unique compliance risk from the perspective of vendors, and those applications and services are

248 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(a)(2).

249 *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(7).

more likely to provide an opportunity to unsubscribe or opt out than for products with only first-party marketing. [250,251]

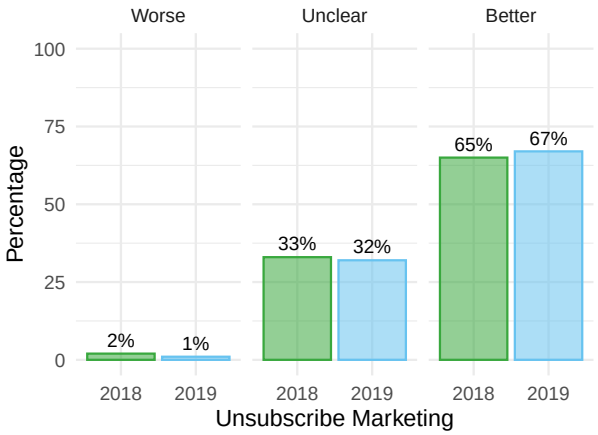


Figure 109: Do the policies clearly indicate whether or not a user can opt out or unsubscribe from a vendor or third party marketing communication?

Compared to 2018, applications and services evaluated in 2019 indicate no meaningful shift in industry behavior. This is likely because the majority of companies that disclose they provide third-party marketing (71%) is within 4% of companies that also disclose that they allow users to unsubscribe or opt out from third-party marketing communications(67%).

Full: Parental Consent

The concern of Parental Consent primarily examines practices where personal information from children under 13 years of age and students are collected, used, or disclosed only with parental consent and methods are available to provide parental consent and withdraw consent.

Parental Consent Scores

Figure 110 illustrates the Parental Consent scores among all applications and services evaluated. Table 22 compares and summarizes the Parental Consent concern score minimum, maximum, median, mean, Q1 (point between the 1st and 2nd quartile), and Q3 (point between the 3rd and 4th quartile).

Table 22: 2018 vs. 2019 Parental Consent score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	0	20	52	48	70	100
2019	0	40	60	54	70	100

From the analysis of 10 related questions in the concern, we determined a median in 2019 of approximately 60%. This median is lower than expected, given these applications and services are intended for children and students and a majority of companies disclose qualitatively better practices that personal information from children and students is only collected with verifiable parental consent.

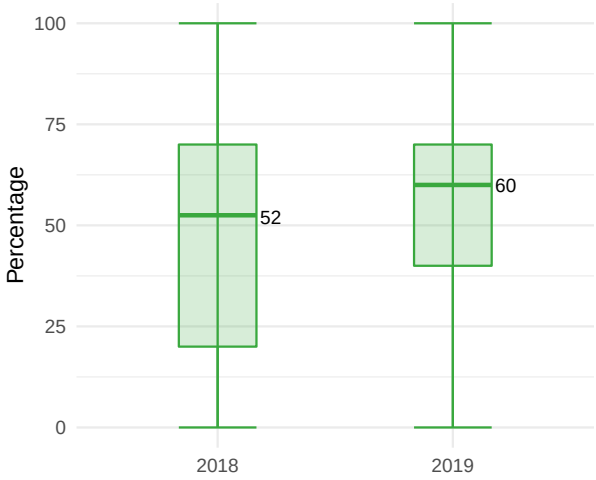


Figure 110: Comparison of Parental Consent scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of Parental Consent indicate a 15% increase in median scores that indicate more transparent and qualitatively better practices of obtaining verifiable parental consent before the collection, use or disclosure of personal information from children or students. In addition, since 2018 the second and third quartiles for Parental Consent have consolidated considerably. However, the statute score still indicates a lack of transparency in companies' policies about parental consent that can create 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 of the compliance obligations required for collecting, using, and disclosing personal information from children and students. This lower concern score is likely 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 nontransparent on all parental

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

251 *See* General Data Protection Regulation (GDPR), Automated individual decision-making, including profiling, Art. 21(2)-(3).

consent-related questions. However, these applications and services likely appeal to children and students under 13 years of age, and are currently among the most popular 150 educational applications and services used by children and students. Also, applications and services are likely to focus their policy disclosures only on compliance obligations that are required to be disclosed, and therefore remain nontransparent about important limitations or exceptions to parental consent.[252,253]

Therefore, applications and services need to provide greater transparency whether they obtain verifiable parental consent. When these practices are not 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 collected in order to meet their expectations of privacy.

Children Intended

Among the applications or services we evaluated, approximately 88% disclosed whether or not the application or service was intended for children under 13 years of age. However, our analysis indicates approximately 12% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 20% of applications and services evaluated indicated the application or service is not intended for children under 13 years of age.

This high percentage of transparent responses is expected given our evaluation process targeted 150 popular edtech applications and services used by children.[254] However, it appears a high percentage of applications and services disclose they are intended for children under 13, but do not also disclose expected compliance obligations for the collection, use, and disclosure of information from those children, as discussed in the COPPA Notice section. In addition, it is unexpected that approximately 20% of applications and services disclose the application or service is not intended for children under 13 years of age. This finding is also observed in the Parental Consent section, where general audience consumer focused applications and services disclose they are not directed or targeted to children under 13 years of age. However, these applications and services likely appeal to children under 13 which take into account several factors, as discussed in the Intended Users section.[255] In addition, many applications and services disclose they are not intended for children under 13 years old, and are only intended for parents and teachers, as discussed in the Parents Intended and Teachers Intended sections, but the product is primarily designed to collect and share personal information, photos, videos, content, and comments about children. As discussed in the COPPA Notice section, this practice allows the vendor to avoid collecting personal information directly *from* children and instead only collect children's personal information indirectly. This practice does not trigger parental consent compliance obligations under COPPA, and the vendor does not need to obtain Actual Knowledge of the age of children that have their content shared in the application or service.

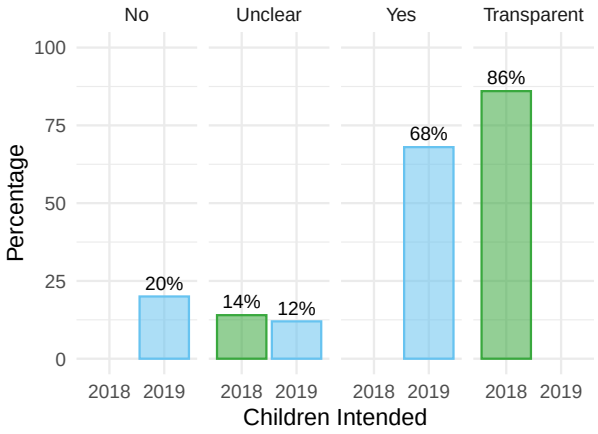


Figure 111: Do the policies clearly indicate whether or not the product is intended to be used by children under the age of 13?

Compared to 2018, applications and services evaluated in 2019 indicate a 2% increase in transparent practices that companies disclose whether or not the application or service was intended for children under 13 years of age. However, as described in the Intended Users section, companies with mixed-audience products that include children, students, parents, teachers, or consumers as their intended users need to carefully describe their data collection and use policies for all users. Lastly, parents and teachers need to exercise extreme caution when evaluating whether to use popular edtech applications or services that indicate they are not intended for children, and companies need to provide greater transparency about their collection, use, and disclosure practices of personal information collected *from* and *about* children under 13 years of age.

Parents Intended

Among the applications and services we evaluated, approximately 52% disclosed a transparent response whether or not the product is intended to be used by parents. However, our analysis indicates approximately 48% of applications and services evaluated are unclear on this issue. In addition, our

252 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(1)-(4).
253 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(6), 99.31(b)(2).
254 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
255 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

analysis indicates approximately 4% of applications and services indicated they are not intended for parents.

This transparent finding is expected given our evaluation process targeted 150 popular edtech applications and services used by children, which often require parents to use the product to create accounts for their children, for parental consent, or child monitoring purposes. However, the high percentage of applications and services that remain non-transparent on this issue are likely because they believe it is self-evident that the product is intended for children and students and do not need to disclose users who are not intended to use the product.

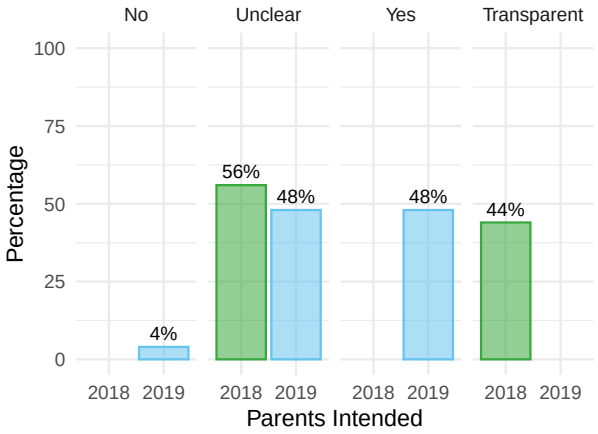


Figure 112: Do the policies clearly indicate whether or not the product is intended to be used by parents or guardians?

Compared to 2018, applications and services evaluated in 2019 indicate an 8% increase in transparent practices that companies disclose whether or not the product is intended to be used by parents. This positive trend is likely the result of companies updating their policies to clarify parents use the application or service to provide parental consent or are required to use the product register an account for their child under 13 years of age.[256] Companies also likely updated their products in 2019 based on increased awareness of digital-well-being concerns of monitoring "screen-time" with more robust features that allow parents to take a more active role in their child's use and control of the application or service; including monitoring activities and academic progress or even engaging in social interactions with their child's teacher.

Actual Knowledge

Among the applications and services we evaluated, approximately 79% disclosed a transparent response whether or not the company has actual knowledge that personal information is collected from children under 13 years of age. However, our analysis indicates approximately 21% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 24% of applications and services evaluated indicate the company does not have actual knowledge that personal information is collected from children under 13 years of age.

This high percentage of transparent responses is expected given our evaluation process targeted 150 popular edtech applications and services used by children. Similarly to the Children Intended concern, companies should disclose their product uses an age-gate or some other account restriction mechanism to determine whether a child under 13 is using the product in order to obtain verifiable parental consent before the collection, use, or disclosure of that child's personal information. In addition, a vendor who obtains actual knowledge that it is collecting information from a child must not encourage that child from disclosing more information than reasonably necessary through an age verification mechanism. Under COPPA, an age gate should be: appropriate for all ages, not encourage falsification, list the day, month, and year, have no prior warning that children under 13 will be blocked, and prevent multiple attempts.[257,258] However, it is unexpected that approximately 25% of applications and services indicate they do not have actual knowledge that personal information is collected from children under 13 years of age. This is likely because general audience applications or services often disclose that children are not the intended users. However, as discussed in the Intended Users section, a general audience product may in fact be considered directed to children under COPPA if the product would appeal to children under 13 years of age, which takes several factors into consideration. Moreover, a similar percentage of applications and services disclosed in the Children Intended section, that children are not the intended users of the product (20%) as disclosed they do not have actual knowledge that children under 13 are using the product (25%).

256 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(2)(i)-(iv); *See also* 15 U.S.C. § 6501(9).

257 *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.3(d).

258 *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.120(d).

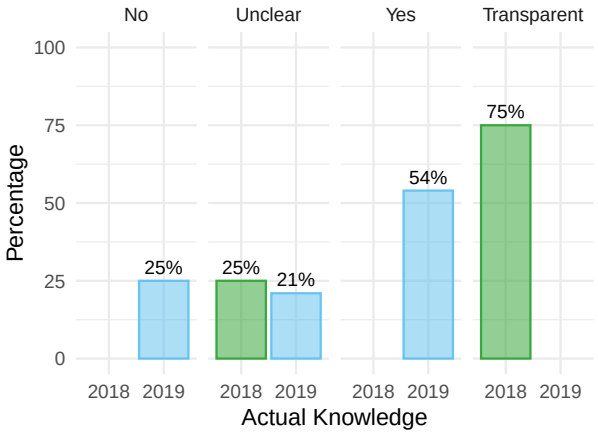


Figure 113: Do the policies clearly indicate whether or not the vendor has actual knowledge that personal information from children under 13 years of age is collected by the product?

Compared to 2018, applications and services evaluated in 2019 indicate a 4% increase in transparent practices that companies disclose whether or not they have actual knowledge that personal information is collected from children under 13 years of age. Similarly to the Children Intended section, this positive trend is likely the result of companies updating their policies to clarify whether the company has actual knowledge that children under 13 years of age are using the application or service in order to meet their compliance obligations under COPPA to contact parents to obtain parental consent.

However, the relative amount of applications and services nontransparent as compared to 2018 is likely the result of companies that enter into contracts with schools and districts and require the school or district to control the collection of personal information from children and students that are under 13 years of age. These companies may assume that because the supplementary contract discloses the school or district faculty control the deployment of the application or service and administration of student accounts of users under 13 years of age, they do not need to disclose that practice in their policies.

COPPA Notice

Among the applications and services we evaluated, approximately 65% disclosed a qualitatively better response that describes how they collect, use, and disclose personal information from children under 13 years of age under COPPA. However, our analysis indicates a significant percentage, of approximately 34% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates a negligible percentage, of approximately 1% of applications and services evaluated discussed qualitatively worse practices that they do not collect, use, and disclose personal information from children under 13 years of age under COPPA.

This qualitatively better finding is expected given our evaluation process targeted 150 popular edtech applications and services used by children. However, approximately 68% of applications and services indicated the product is intended for children under 13 years of age, but do not also disclose compliance obligations for the collection, use, and disclosure of information from those children.[259] Given that approximately 32% disclosed the application or service is not intended for children or are unclear about whether or not children are intended users, as seen in the Children Intended section, it is not surprising to see 34% of policies are unclear with respect to providing COPPA notice.

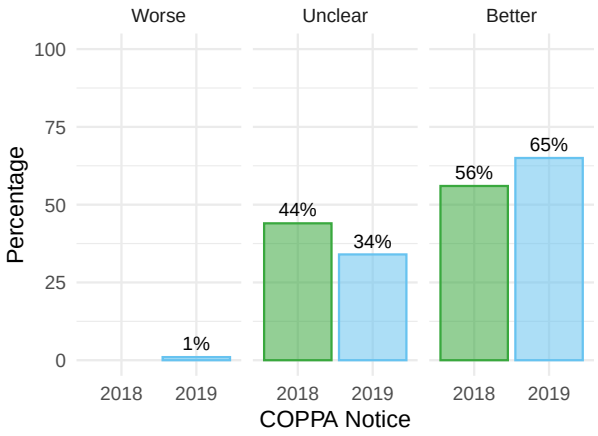


Figure 114: Do the policies clearly indicate whether or not the vendor describes: (1) what information is collected from children under 13 years of age, (2) how that information is used, and (3) its disclosure practices for that information?

Compared to 2018, applications and services evaluated in 2019 indicate a 9% increase in qualitatively better practices that companies describe how they collect, use, and disclose personal information from children under 13 years of age. In addition, since 2018 there has been a respective 10% decrease in unclear practices. Similarly to the Children Intended section, this positive trend may be the result of companies updating their policies to clarify whether the application or service is intended for children under 13 years of age in order to meet their compliance obligations under COPPA to contact parents to obtain parental consent.

However, applications and services with unclear practices are likely related to the 20% of vendors who disclose their

[259] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.3(a), 312.4(d), 312.4(d)(2).

products are not intended for children or students and companies that enter into private contracts with schools and districts that require the school or district to control the collection, use, and disclosure of personal information from children and students that they determine are under 13 years of age. However, products not intended for children may still be considered directed to children if the product would appeal to children under 13 years of age, which takes several factors into consideration such as: the subject matter, visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the product, or whether advertising promoting or appearing on the product is directed to children.

COPPA Exception

Among the applications and services we evaluated, approximately 15% disclosed that they collect personal information from children without verifiable parental consent, but for the sole purpose of obtaining consent. However, our analysis indicates a significant percentage, of approximately 78% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 7% of applications and services evaluated discussed that they do not collect personal information from children without verifiable parental consent.

This significant unclear finding is likely the result of the majority of applications and services evaluated not collecting, using, or disclosing personal information from children under 13 years old without parental consent, as described in the Parental Consent section; with approximately 72% disclosing they obtain parental consent. Therefore, these applications and services are not required to disclose exceptions to obtaining parental consent under COPPA, because they do not engage in those practices. However, as described in the Delete Child-PII section, approximately 50% of applications disclose they delete personal information collected from children under 13 years old unless parental consent was obtained, which means they engage in practices that are exceptions provided by COPPA. Moreover, at least 28% of applications and services that disclose they delete personal information from children obtained without consent (50%), do not also disclose they provide exceptions under COPPA for collecting that personal information from children for the purposes of obtaining consent (78%) and whether additional protections are put in place to protect a child or students' personal information before parental consent is obtained.[260] When practices that companies engage in are not 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 obtain parental consent and meet their expectations of privacy.

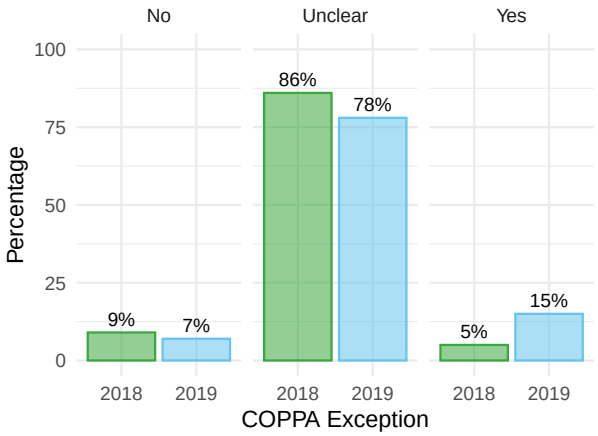


Figure 115: Do the policies clearly indicate whether or not the vendor collects personal information from children without verifiable parental consent for the sole purpose of trying to obtain consent under COPPA?

Compared to 2018, applications and services evaluated in 2019 indicate a 10% increase in companies that indicate they collect personal information from children without verifiable parental consent, but only for the purpose of obtaining consent. In addition, since 2018 there has been a respective 8% decrease in unclear practices. Similarly to the Children Intended section, this positive trend may be the result of companies updating their policies to clarify whether or not the application or service is intended for children under 13 years of age in order to meet their compliance obligations under COPPA and disclose exceptions provided by COPPA to collect personal information from children in order to contact parents to obtain parental consent.

Parental Consent

Among the applications or services we evaluated, approximately 73% disclosed qualitatively better practices that verifiable parental consent must be obtained before they collect, use, or disclose any child or student's personal information. However, our analysis indicates approximately 24% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 3% of applications and services evaluated discussed qualitatively worse practices that verifiable parental consent is not obtained before they collect, use, or disclose any child or student's personal information.

This qualitatively better finding is lower than expected, perhaps nontransparent applications and services assume they do not need to obtain parental consent if they disclose their

[260] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.5(c)(1)-(4), (7).

service is not intended for children or students. However, a similar percentage (66%) of applications and services are directed to schools, as indicated in the School Purpose section, which likely means nontransparent responses about parental consent may be attributable to additional student data privacy agreements that exist privately between the company and schools or districts that define the verifiable parental consent collection process on behalf of the schools or districts.

In addition, as indicated in the Children Intended section, approximately 32% were either unclear (12%) or indicated they are not intended for kids under 13 (20%), and therefore may claim they are neither directed nor targeted to children under 13 years of age. COPPA requires applications and services obtain parental consent 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 applications or services would still need to obtain parental consent, because they would likely appeal to children under the age of 13, which take into account several factors, as described in the Intended Users section, including that they are among 150 of the most popular edtech products used by children and students.

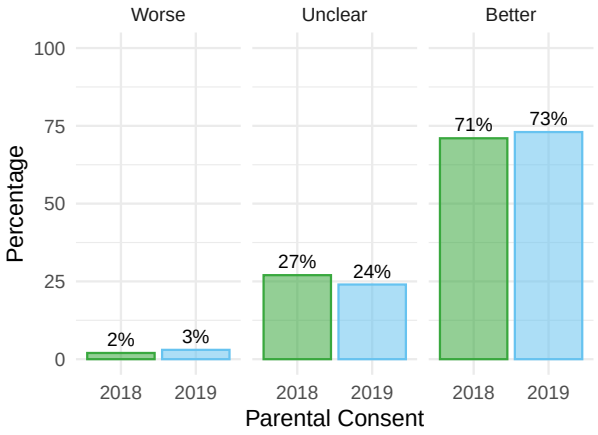


Figure 116: Do the policies clearly indicate whether or not the vendor or third party obtains verifiable parental consent before they collect or disclose personal information?

Compared to 2018, applications and services evaluated in 2019 indicate a marginal 2% increase in qualitatively better practices that verifiable parental consent is obtained before they collect, use, or disclose personal information. In addition, since 2018 there has been a respective 3% decrease in unclear practices. Similarly to the Children Intended section, this slight positive trend may be the result of companies updating their unclear policies to meet their compliance obligations under COPPA that verifiable parental consent is obtained.

As indicated in both the Children Intended and Students Intended sections, it is assumed approximately 32%, and 29% respectively of nontransparent 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 may be 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 state or federal law.[261,262,263]

Limit Consent

Among the applications and services evaluated that require Parental Consent for the collection or disclosure of information from children or students, approximately 15% disclosed qualitatively better practices that consent to the collection and use of the child's personal information may be independent to consent for the disclosure of information to third parties. However, our analysis indicates approximately 83% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 2% of applications and services evaluated discussed qualitatively worse practices that they do not allow consent to the collection of the child or student's personal information to be independent to consent to share personal information with third parties.

Accordingly, limiting parental consent only 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, and consent for use should be independent to consent to share with third parties. Under COPPA, 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

261 Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.3(d), 312.5, 312.5(a), 312.5(b)(1)-(2)(i)-(iv); *See* 15 U.S.C. § 6501(9).

262 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

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

use of their child's personal information, without also consenting to the disclosure of that information to third parties for the vendor or third-party's own purposes.[264]

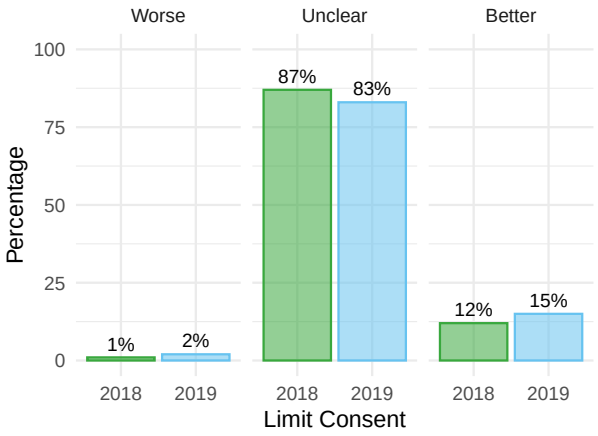


Figure 117: Do the policies clearly indicate whether or not a parent can consent to the collection and use of their child's personal information without also consenting to the disclosure of the information to third parties?

Compared to 2018, applications and services evaluated in 2019 indicate a 3% increase in qualitatively better practices that they allow consent to collect versus consent to share personal information with third parties to independently managed. In addition, since 2018 there has been a respective 5% decrease in unclear practices. Similarly to the Parental Consent section, this slight positive trend may be the result of companies updating their policies to meet their compliance obligations under COPPA that verifiable parental consent is obtained and limited with respect to disclosure to third parties.

However, our findings indicate that the majority of applications and services disclose they obtain parental consent, as discussed in the Parental Consent section, but have unclear practices limiting consent which indicates parental consent is not properly bifurcated, assuming personal information is collected and shared. Applications and services with unclear practices effectively treat parental consent as a universal green light that any collected information can 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 consenting to disclose that information to third parties. For example, our previous analysis found in the Data Shared section that approximately 96% of applications and services share personal information with third parties. In addition, our previous findings determined shared information is commonly used for advertising and marketing purposes, as described in the Third-Party Marketing, Traditional Advertising, and Behavioral Advertising sections. 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 and avoid potential compliance issues under COPPA.

Withdraw Consent

Among the applications and services evaluated that require Parental Consent for the collection or disclosure of information from children or students, approximately 47% disclosed a qualitatively better response that they respond to requests from parents or guardians to prevent further collection of their child or student's information. However, our analysis indicates approximately 53% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates no applications and services evaluated discussed that they do not respond to a request from a parent or guardian to prevent further collection of their child or student's information.

This unclear finding is likely the result of applications and services simply stopping collection of personal information from children and students when they no longer use the product or delete their data or account. Practically speaking, when a child or student chooses to no longer use a product and no longer provide their personal information, the company should understand that choice to mean they have effectively withdrawn consent for the further collection of personal information, because no more personal information should be collected. As a result, companies may believe they do not need to disclose self-evident practices in their policies that when a user stops using the product without notice they have withdrawn consent for further collection of data. However, this assumption of how withdrawing consent works by companies is incorrect because it does not take into account that when a parent or educator provides notice to a company to prevent further collection of their child or students' personal information by an application or service, that withdrawal also applies retroactively to the consent given for all previously collected personal information–not just to the future collection and use of information.[265]

As discussed in the Parental Consent section, if there is no parental consent for the collection, use, or disclosure of personal information from children under 13 years of age, then that information must be deleted as discussed in the Delete Child-PII section. However, when personal information is collected with parental consent, but then parental consent

[264] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(a)(2).

[265] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.3(c), 312.4(d)(3), 312.6.

is later withdrawn, there is no legal basis for the vendor to continue processing the previously collected personal information because the purpose in which the information was collected to provide the services can no longer be provided; as the children or students are no longer using the services and the information should be deleted as a best practice, as discussed in the Retention Policy section. Parental consent may be withdrawn for a specific practice such as sharing personal information with third parties, as discussed in the Limit Consent section, but not for other practices such as the collection and use of information by the vendor to continue providing the service to the child or student. Therefore, it is important that vendors increase their transparency on the methods in which parents and guardians can provide verifiable parental consent, as discussed in the Consent Method section, because it allows more notice and choice to provide or withdraw consent, and the vendor obtains verifiable compliance certainty when consent is withdrawn and for what purpose rather than assuming consent is withdrawn when the child or student stops using the service.

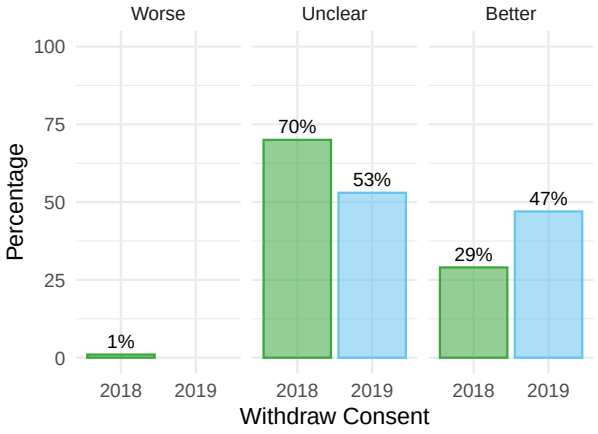


Figure 118: Do the policies clearly indicate whether or not the vendor responds to a request from a parent or guardian to prevent further collection of their child's information?

Compared to 2018, applications and services evaluated in 2019 indicate an 18% increase in qualitatively better practices that companies disclose they respond to requests from parents or guardians to prevent further collection of their child's information. This positive trend is likely the result of companies updating their policies for compliance purposes to incorporate new privacy rights granted by changing International and U.S. state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018 and provided many new privacy rights for company's subject to the GDPR's requirements including the right to withdraw consent at any time.[266]

[266] *See* General Data Protection Regulation (GDPR), Art. 7(3), 13(2)(c), 14(2)(d), 17(1)(b).

Delete Child PII

Among the applications and services evaluated, approximately 50% disclosed they delete personal information from a child or student under 13 years of age if collected without parental consent. However, our analysis indicates approximately 49% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 1% of applications and services evaluated discussed qualitatively worse practices that they do not delete personal information from a child or student under 13 years of age if collected without parental consent.

Accordingly, deleting a child's personal information if collected without parental consent is considered a qualitatively better practice in our evaluation process, because it prevents personal information from children being used in unexpected ways without informing a parent or guardian and is a requirement to remain in compliance with federal law.[267] This otherwise large percentage of unclear responses is not surprising given that approximately 73% of applications and services, as indicated in Parental Consent, disclose parental consent is required prior to the collection of personal information. However, this compliance practice is intended to mitigate potential liability if the application or service manages the parental consent process itself or to mitigate potential compliance liability if teachers and schools are unable to produce verifiable records that parental consent was obtained on the vendor's behalf as would be necessary for the 54% of applications and services indicated in the School Consent section, that transfer parental consent to the school or district. However, applications and services with unclear responses 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. Applications and services that disclose parental consent is required, but are unclear about how child or student data is handled without verifiable consent, are likely to lose adoption among parents, teachers, schools, and districts. Without proper consent there is an increased risk for potential misuse and unauthorized disclosure of child and student information to third parties.[268,269]

[267] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(1).

[268] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.6(c).

[269] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

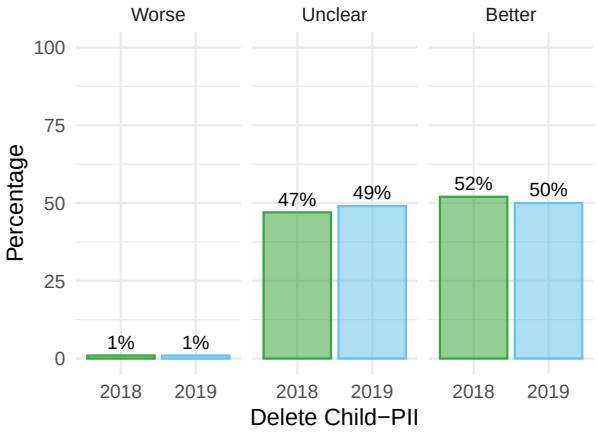


Figure 119: Do the policies clearly indicate whether or not the vendor deletes personal information from a student or child under 13 years of age if collected without parental consent?

Compared to 2018, applications and services evaluated in 2019 indicate a 2% decrease in qualitatively better practices that companies disclose they delete personal information from a child or student under 13 years of age if collected without parental consent. This slight, seemingly negative trend may be the result of an increase, as described in the Parental Consent section, in qualitatively better practices that applications and services are obtaining parental consent before the collection, use, or disclosure of personal information from children or students under 13. Therefore, companies may be updating their policies to remove this practice given they have a more strict parental consent mechanism in place to prevent the inadvertent collection of personal information from children without prior parental consent. However, companies should include this practice in their policies, even if the likelihood of collecting personal information from children without consent is low, because there may be a technical or human error that results in the inadvertent collection of a child's personal information. Additionally when practices that protect children's personal information are not 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 without consent in order to meet their expectations of privacy.

Consent Method

Among the applications and services evaluated, approximately 42% disclosed qualitatively better practices of the methods available for parents or guardians to provide verifiable parental consent. However, our analysis indicates approximately 55% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 3% of applications and services evaluated discussed qualitatively worse practices that they do not provide methods for parents or guardians to provide verifiable parental consent.

This qualitatively better finding is comparatively low given these applications and services are intended for children under 13 years of age and students. From our analysis this unclear percentage is nonconforming with the Children Intended section, that indicates approximately 68% of applications and services evaluated are intended for children under 13 years of age, and with the Parental Consent section, that indicates approximately 72% of applications and services disclosed they obtain parental consent. However, our findings indicate applications and services that are unclear about the methods available to provide parental consent, may provide a secondary "Parent" or "Teacher" account that use online methods to provide consent through the creation of an associated child or student account. Approximately 55% of applications and services are unclear on this issue, but 48% disclose they are intended for parents, and 69% are intended for teachers, as respectively seen in the Parents Intended and Teachers Intended sections. This discrepancy may be because vendors assume the implication of having a parent or teacher account is adequate disclosure of the process or method of obtaining verifiable consent. However, the process or method of obtaining verifiable parental consent cannot be implied by the presence of a parent or teacher account, and a verifiable consent method can be a separate process that may not require a parent or teacher to create an account with the application or service. Therefore, vendors need to increase their transparency on this important issue, because if it is not clear how parents and teachers can provide verifiable consent but the product can still be used without consent, then children and students are at a greater risk of their information being collected, used, and disclosed without verifiable consent and vendors may be in violation of the law.

However, these parent or teacher accounts could potentially be used as a means to collect personal or behavioral related information from the parents and teachers themselves, as described in the Intended Users section. 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 disclose the various methods that are 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.[270]

[270] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(1)-(2)(i)-(vi).

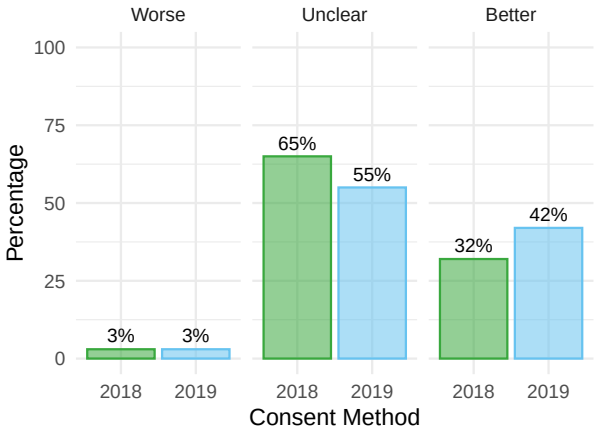


Figure 120: Do the policies clearly indicate whether or not the vendor provides notice to parents or guardians of the methods to provide verifiable parental consent under COPPA?

Compared to 2018, applications and services evaluated in 2019 indicate a 10% increase in qualitatively better practices that companies disclose the methods available for parents or guardians to provide verifiable parental consent. This positive trend is likely the result of companies updating their policies for compliance purposes to incorporate new privacy rights granted by changing International and U.S. state privacy laws. For example, Europe's General Data Protection Regulation (GDPR) came into effect in May 2018 and provided many new privacy rights for people subject to the GDPR's requirements including the right to withdraw consent at any time which requires additional disclosures in a company's policies about the methods in which to provide and withdraw consent.[271]

Full: School Purpose

The concern of School Purpose primarily examines practices of applications and services primarily used for K-12 school purposes with students and teachers where personal information from students is used to create educational records and third-party companies serve as "School Officials" to a school or district.

School Purpose Scores

Figure 121 illustrates the School Purpose scores among all applications and services evaluated. Table 23 compares and summarizes the School Purpose concern score minimum, maximum, median, mean, Q1 (point between the 1st and 2nd quartile), and Q3 (point between the 3rd and 4th quartile).

Table 23: 2018 vs. 2019 School Purpose score descriptive statistics

	Min.	Q1	Med.	Mean	Q3	Max.
2018	10	18	45	41	56	85
2019	10	26	50	46	65	85

From the analysis of 10 related questions in the concern, we determined a median in 2019 of approximately 50%. This median is lower than expected, given these applications and services are intended for children and students and a majority of companies disclose qualitatively better practices that student personal information is only collected for the educational purpose of providing the application or service.

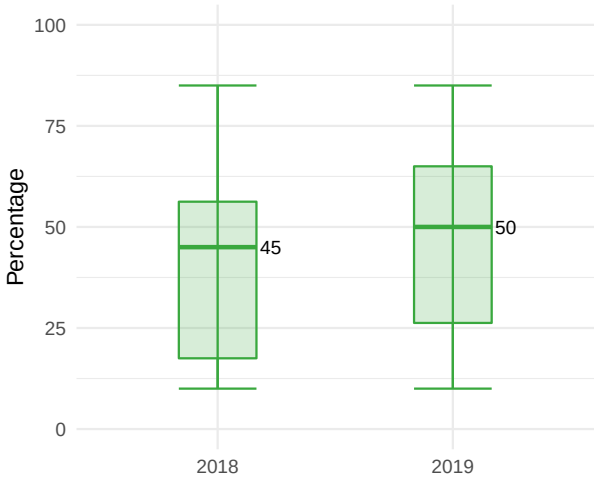


Figure 121: Comparison of School Purpose scores year over year

Compared to 2018, applications and services evaluated in 2019 for the concern of School Purpose indicate an 11% increase in median scores that indicate more transparent and qualitatively better practices of protecting personal information collected from students for an educational record. However, this lower concern score finding is likely the result of companies that enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent requests to access and review that data from eligible students, teachers, and parents. These companies may assume that because the contract discloses the school or district faculty control the deployment of the application or service and administration of student accounts they do not also need to disclose those practices in their publicly available policies.

271 *See* General Data Protection Regulation (GDPR), Conditions Applicable to Child's Consent in Relation to Information Society Services, Art. 8(2)

Students Intended

Among the applications or services we evaluated, approximately 71% disclosed that the applications or services evaluated are intended for students. However, our analysis indicates approximately 26% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 3% of applications and services evaluated disclosed their products are not intended for students.

This high percentage of transparency is expected given our evaluation process targeted 150 popular edtech applications and services used by students in the classroom. Moreover, our unclear finding is not unexpected because 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. Given that we see 29% are either explicitly not intended for kids or unclear whether or not kids are intended, teachers should exercise additional caution prior to using applications or services that fall into this category to ensure that all the necessary protections are in place since the vendor has not considered or has specifically indicated they are not intended for these use cases. The approximately 14% percent greater occurrence of unclear responses to this question, as compared to the Children Intended section, may be attributable to applications and services disclosing they are only intended for children, because they are under the assumption use by children inherently includes educational use. 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 of personal information from students.[272,273,274]

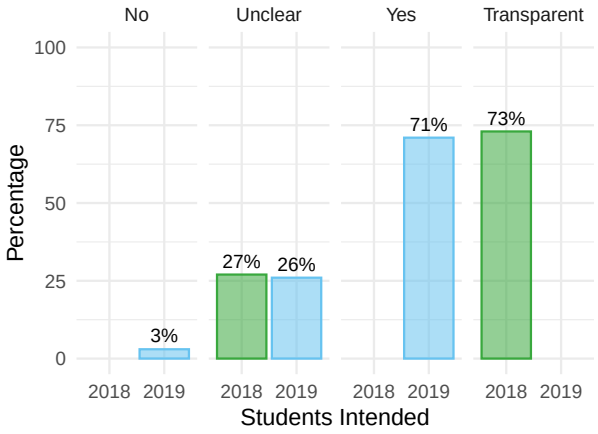


Figure 122: Do the policies clearly indicate whether or not the product is intended to be used by students in preschool or K-12?

Compared to 2018, applications and services evaluated in 2019 indicate no change in transparent disclosures that students are intended users. In addition, since 2018 our findings indicate a plateau with a 1% decrease in unclear practices, and 2% increase in transparent disclosure that students are not intended users. However, as described in the Intended Users section, companies with mixed-audience products that include children, students, parents, teachers, or consumers as their intended users need to carefully their data collection and use policies for all users. Lastly, parents and teachers need to exercise caution when evaluating whether to use popular edtech applications or services that disclose they are not intended for children as their may not be adequate protection or consideration of students, and companies need to provide greater transparency about their collection, use, and disclosure practices of personal information from students.

Student Data

Among the applications and services we evaluated, approximately 60% disclosed a qualitatively worse response that the company collects personal information or education records from preK-12 students. However, our analysis indicates approximately 35% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 5% of applications and services evaluated discussed qualitatively better practices that the company does not collect personal information or education records from preK-12 students.

This qualitatively worse finding is likely the result of applications and services collecting personal information from students in order to provide the services. The collection of personal information from students is not always necessary in order to use the application or service as intended, and is considered a worse practice as the collection of personal

272 Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(a), 22584(m); *See* 22586(a)(1).

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

274 *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.6.

information and education records from students increases the risk that the information may inappropriately be used or disclosed. Collection of personal information and education records also raises additional compliance challenges for vendors regarding the use, protection, and disclosure of that personal information to third parties.[275,276] For the purposes of this evaluation, we recommend that applications and services intended for students not collect any personal information or education records if possible, as described in the School Contract section, or limit their collection of information as described in the Collection Limitation section.

From our analysis, it appears there is approximately an 11% lower occurrence in the disclosure of transparent practices of collecting student data (60%), as compared to the percentage of applications intended for students (71%), as indicated in the Students Intended section. This is likely the result of companies disclosing the application or service is intended for students, but not disclosing any additional information about the collection, use, or disclosure of student data because of additional contracts entered into with schools and districts. Companies enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent requests to access and review that student data from eligible students, teachers, and parents. These companies may assume that because the private contract discloses the school or district faculty control the deployment of the application or service and administration of student accounts they do not also need to disclose that practice in their publicly available policies.

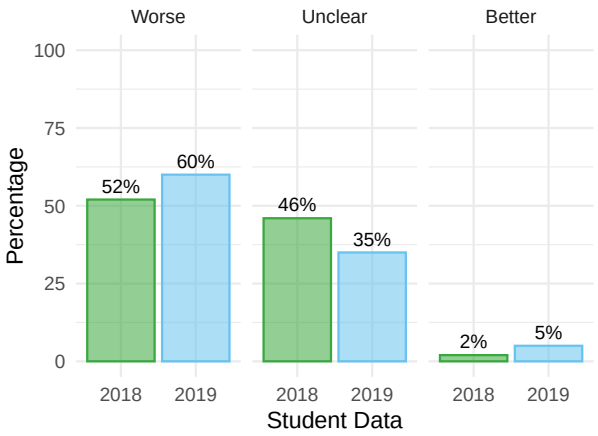


Figure 123: Do the policies clearly indicate whether or not the vendor collects personal information or education records from preK-12 students?

Compared to 2018, applications and services evaluated in indicate a positive trend with an 11% decrease in unclear practices, but unfortunately most of those gains were accounted for in an 8% increase in qualitatively worse practices indicating that they collect personal information or education records. Similarly to decreases in unclear practices in the School Purpose section, this is likely the result of companies updating their policies for compliance purposes to clarify distinctions between student data and different privacy rights granted by changing International and U.S., state privacy laws.[277]

Teachers Intended

Among the applications and services we evaluated, approximately 69% disclosed that the product is intended to be used by teachers. However, our analysis indicates approximately 31% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 0% of applications and services evaluated disclosed that the product is intended to be used by teachers. Also, since 2018 this question format changed but the data can still be compared in a transparent or nontransparent format. below.

This high transparent finding is expected given our evaluation process targeted 150 popular edtech applications and services used by students, which often requires educators to use the product to create and manage accounts for their students, for obtaining parental consent, or student assessment purposes.[278,279,280,281] However, the high percentage of applications and services that remain unclear on this issue may be because they believe it self-evident that the product is not intended for teachers to be used in K-12 classrooms and therefore they do not need to disclose users who are not intended to use the product.

275 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

276 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(a); *See also* § 22586(a)(1).

277 Future of Privacy Forum (FPF), *The Policymaker's Guide to Student Data Privacy* (Apr. 4, 2019), https://ferpasherpa.org/wp-content/uploads/2019/04/FPF-Policymakers-Guide-to-Student-Privacy-Final.pdf.

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

279 *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(a); *See also* § 22586(a)(1).

280 *See* Protection of Pupil Rights Act (PPRA), 34 C.F.R. § 98.3.

281 *See* California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code §§ 49073.1.

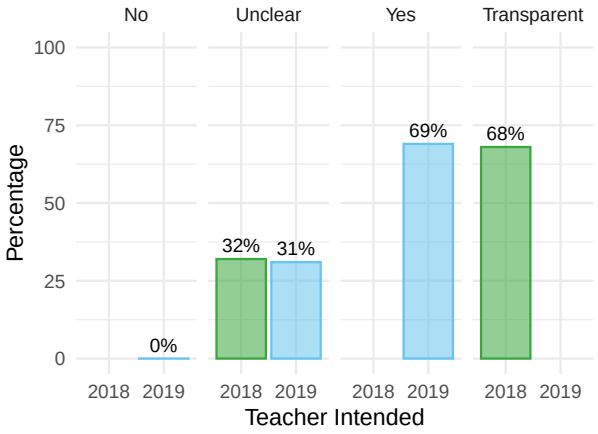


Figure 124: Do the policies clearly indicate whether or not the product is intended to be used by teachers?

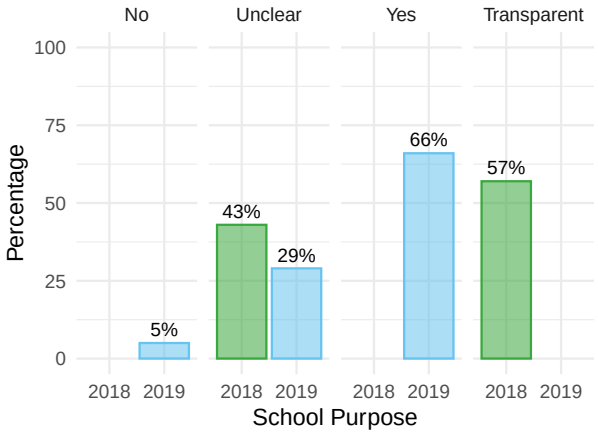


Figure 125: Do the policies clearly indicate whether or not the product is primarily used, designed, and marketed for preschool or K-12 school purposes?

Compared to 2018, applications and services evaluated in 2019 indicate no change in practices that the product is intended to be used by teachers. This plateau is likely the result of applications and services assuming it may be obvious teachers are not intended users.

School Purpose

Among the applications or services we evaluated, approximately 66% disclosed that the applications or services are primarily designed, marketed, and used for preschool or K-12 school purposes. However, our analysis indicates approximately 29% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 5% of applications and services evaluated disclosed the applications or services are not primarily designed, marketed, and used for preschool or K-12 school purposes.

However, in the Students Intended section, there is a higher occurrence of approximately 5% between applications and services that disclose 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 disclose they are intended for students, but only target higher education students over 18 years of age or would be considered homework or self-study products intended for use outside a K-12 school environment. 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).[282]

[282] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(a), 22584(m), 22586(a)(1).

Compared to 2018, applications and services evaluated in 2019 indicate a positive 14% decrease in unclear practices that do not disclose whether or not the products is primarily designed, marketed, and used for preschool or K-12 school purposes. This finding is likely the result of companies updating their policies for compliance purposes to clarify distinctions between student data and different privacy rights granted by changing International and U.S. state privacy laws.

Education Records

Among the applications or services we evaluated, approximately 60% disclosed the process by which education records are entered into the product. However, our analysis indicates approximately 40% of applications and services evaluated do not indicate how education records are entered into the product.

Accordingly, education records are information that is directly related to a student and maintained by an educational institution and therefore it is not surprising that a similar percentage of applications and services disclose in the Student Data section, that they both collect personal information from students and describe the additional protections and rights for parents to review and correct education records that are entered into the product.[283,284]

[283] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1, 99.3.

[284] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(o)(1)(J).

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

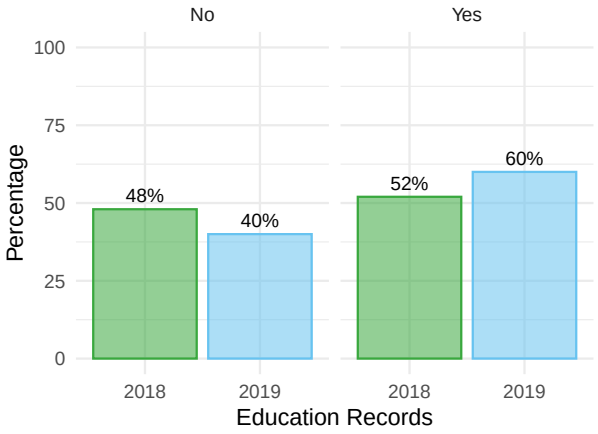


Figure 126: Do the policies clearly indicate the process by which education records are entered into the product? For example, are data entered by district staff, school employees, parents, teachers, students, or some other person?

Compared to 2018, applications and services evaluated in 2019 indicate a positive 8% increase in practices that disclose the process by which education records are entered into the product. In addition, since 2018 there has been a respective 8% decrease in unclear practices. This finding may be the result of companies updating their policies for compliance purposes to clarify distinctions between student data and data created for educational purposes and maintained by the school or district as education records. If the school or district enters into a contract with a company to provide services to its students, these agreements typically require a school or district representative to respond to requests directly from parents and teachers on behalf of students to access, modify, or delete student education records.

School Contract

Among the applications and services we evaluated, approximately 37% disclosed a qualitatively better response that the company provides a contract or student data privacy agreement to a local education agency to protect student data. However, our analysis indicates approximately 61% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 2% of applications and services evaluated discussed qualitatively worse practices that the company does not provide a contract or student data privacy agreement to a local education agency to protect student data.

As described in the School Purpose and Students Intended sections, approximately 66% and 71% respectively disclose that the applications or services are intended for students and primarily designed, marketed, and for preschool or K-12 school purposes. Accordingly, a contract or student data privacy agreement with a local education agency to protect student data is only required in situations when a company's publicly available policies are inadequate to protect the privacy and security of student data, or the school or district needs to clearly define the company's compliance obligations and places them under the direct control of the educational institution as a School Official.[285,286,287] Companies that disclose that the applications or services are intended for students and primarily designed, marketed, and for preschool or K-12 school purposes, but are unclear on this issue, perhaps because they believe their policies sufficiently protect student data. However, as described in the School Purpose Scores section, we determined a median in 2019 of approximately 50%. This median is lower than expected, given these applications and services are intended for children and students and a majority of companies disclose qualitatively better practices that student personal information is only collected for the educational purpose of providing the application or service.

Negotiated student data privacy agreements serve to fill this gap between a school or district's privacy expectations and the company's publicly available privacy policies. Companies often enter into contracts with schools and districts and require the school or district to control the collection of personal information and subsequent requests to access and review that data from eligible students, teachers, and parents. In addition, these agreements often provide additional student data privacy and security protections that are not disclosed in a company's publicly available policies and that may be required by state law. Student data privacy agreements are also beneficial for schools and districts who are ultimately responsible for "direct control" over the first-party applications and services used by students, as described in the School Official section, and they require knowledge of which third-party service providers are also handling students' personal information so appropriate flow down clause contractual obligations can be put in place on additional third parties. However, companies likely assume that because student data privacy agreements provide additional details requested by the school or district and disclose the school or district faculty control the deployment of the application or service and administration of student accounts, they do not need to disclose that schools or districts can enter into contracts with the company in their publicly available policies. However, when vendors do not transparently disclose that additional student data privacy agreements can be put in place, there is no future expectation or trust on behalf of schools or districts about how collected information from

285 *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.7(a).

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

287 *See* General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art. 13(2)(e).

students will be protected in order to meet their expectations of privacy based only the publicly available privacy policy.[288]

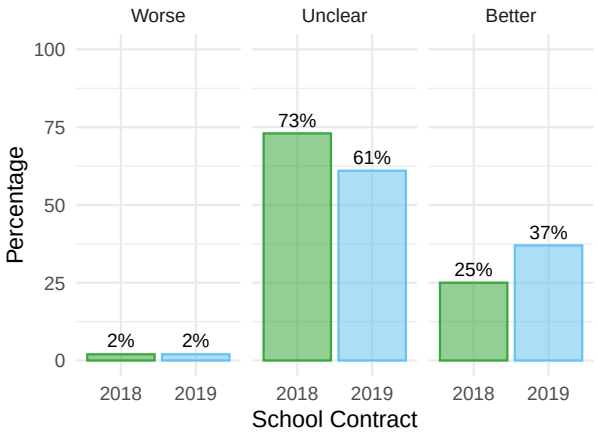


Figure 127: Do the policies clearly indicate whether or not the vendor provides a contract to a Local Educational Agency (LEA) or otherwise provides notice to users of additional rights?

Compared to 2018, applications and services evaluated in 2019 indicate a positive 12% increase in application or services that provide a contract or student data privacy agreement to a local education agency or otherwise provides notice to users of additional rights. In addition, since 2018 there has been a respective 12% decrease in unclear practices. This finding is the result of companies updating their policies for compliance purposes to clarify that they will provide a contract or student data privacy agreement to a local education agency to protect student data. Additionally, if the school or district enters into a contract or agreement with a company to provide services to its students, these agreements typically require a school or district representative to respond to requests directly from parents and teachers on behalf of students to access, modify, or delete student education records.

School Official

Among the applications and services we evaluated, approximately 27% disclosed qualitatively better practices that they operate under the direct control of the educational institution and are designated a School Official under FERPA. However, our analysis indicates approximately 69% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 4% of applications and services evaluated discussed qualitatively worse practices that the company does not operate under the direct control of the educational institution and are not designated a School Official under FERPA.

Accordingly, schools must have written permission from the parent, or 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 that intend to transfer this obligation should enter into contractual relationships with applications and services that designate the vendor as a School Official, as described in the School Contract section, 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 specifying the use of collected information only for educational purposes, as well as describing the process of obtaining parental consent. Accordingly, approximately 69% of applications and services evaluated were unclear on this issue, although approximately 71% disclosed they are intended for students in the Students Intended section, and 66% disclosed they are intended for a School Purpose, in which they are primarily designed, marketed, and used for preschool or K-12 school purposes.

It appears there is approximately a 10% lower occurrence of qualitatively better practices, as compared to the School Contract section, which indicates a moderate percentage of companies are already disclosing in their policies that the company provides a contract (37%) or student data privacy agreement to a local education agency to protect student data, but not that they can also serve as a School Official (27%).

[288] Kelly, G., *Privacy Evaluation of Top 10 District-wide EdTech Products*, Common Sense Privacy Program, (Dec. 21, 2018) https://www.commonsense.org/education/articles/privacy-evaluation-of-top-10-district-wide-edtech-products.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

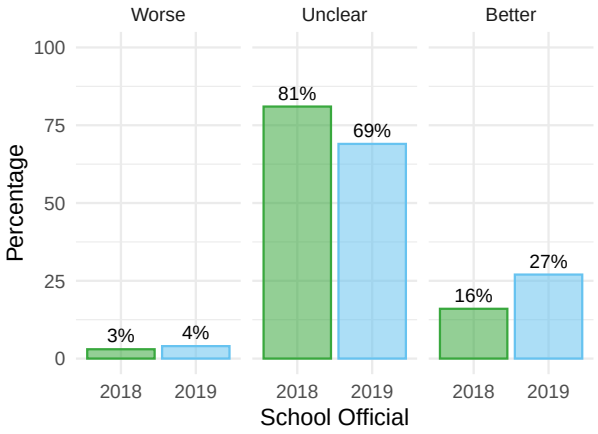


Figure 128: Do the policies clearly indicate whether or not the vendor is under the direct control of the educational institution and designates themselves a School Official under FERPA?

Compared to 2018, applications and services evaluated in 2019 indicate a positive 11% increase in qualitatively better practices that disclose the company will operate under the direct control of the educational institution and are designated a School Official under FERPA. In addition, since 2018 there has been a respective 11% decrease in unclear practices. This finding is likely the result of companies updating their policies for compliance purposes to clarify that they will provide a contract or student data privacy agreement to a local education agency to protect student data and as part of that contract or student data privacy agreement the application or service will be under the direct control of the school or district if serving in the capacity of a School Official. 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.[289] 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, as described in the School Contract section. Templates of student data privacy agreements should be made publicly available when possible 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 a school official, based on the appropriate Federal and State privacy and security protections provided in the agreement.[290,291]

School Consent

Among the applications and services evaluated, approximately 54% disclosed qualitatively worse practices that the responsibility or liability for obtaining verified parental consent is transferred to the school or district. However, our analysis indicates approximately 44% of applications and services evaluated are unclear on this issue. In addition, our analysis indicates approximately 2% of applications and services evaluated discussed qualitatively better practices that they do not transfer the responsibility or liability for obtaining verified parental consent to the school or district.

This qualitatively worse disclosure is alarming, 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, this significant finding may be because there is an exception to the requirement that the application or service itself must obtain verifiable parental consent. As the Federal Trade Commission (FTC) explains, COPPA allows schools to act as an intermediary for parental consent or the parent's agent in the process of collecting personal information from students. 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 educational benefit of the school or district.[292] Therefore, 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.

From our analysis, our findings indicate 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, as discussed in the School Contract section, it effectively exculpates these vendors from any parental consent compliance obligations and responsibilities. As such it is critical for the school or district to ensure verifiable parental consent is properly obtained. By shifting the process of obtaining parental consent to the teacher, school or district, the application or service no longer needs

289 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.7(a).

290 Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(A)-(B), 99.31(a)(1)(ii).

291 California AB 1584 - Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(8).

292 *See* FTC, *Complying with COPPA: Frequently Asked Questions, M. COPPA and Schools*, (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

to determine whether its users are children under the age of 13, as described in the Actual Knowledge section, and can defer to the school or district as the custodian of verifiable parental consent information. Therefore, these applications and services can claim they have no actual knowledge 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, under the assumption that the school or district controls the method of obtaining parental consent, but the vendor can also request to verify that parental consent has been obtained by the school or district.

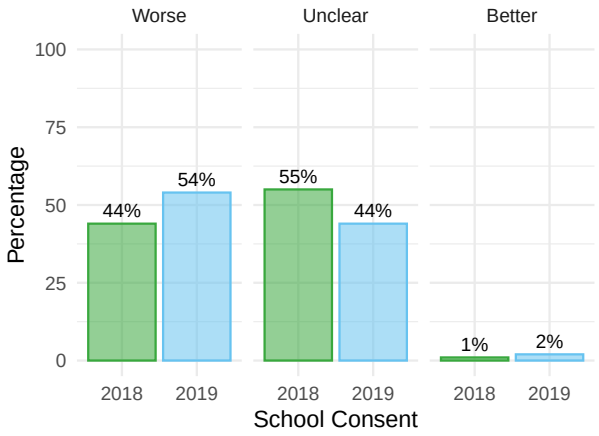


Figure 129: Do the policies clearly indicate whether or not responsibility or liability for obtaining verified parental consent is transferred to the school or district?

Compared to 2018, applications and services evaluated in 2019 indicate a 10% increase in qualitatively worse practices that disclose the compliance obligation to obtain verifiable parental consent is transferred to the teacher, school, or district. In addition, since 2018 there has been a respective 11% decrease in unclear practices. In addition, 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, where approximately 72% disclose 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 43% 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 may be unclear about the methods in which to provide consent; ostensibly to avoid implementing technological methods for the consent collection and verifiable process, which places compliance burdens and penalties for non-compliance on teachers, schools, and districts.

FERPA Exception

Among the applications and services we evaluated, approximately 7% indicated that they disclose personal information from students without verifiable parental consent under a FERPA exception. However, our analysis indicates a significant percentage, approximately 89% of applications and services evaluated, are unclear on this issue. In addition, our analysis indicates approximately 4% of applications and services evaluated discussed that they do not disclose personal information from students without verifiable parental consent under a FERPA exception.

This significant unclear finding is likely the result of the majority of applications and services evaluated simply not collecting, using, or disclosing personal information from students without parental consent, as described in the Parental Consent section; with approximately 72% disclosing they obtain parental consent. There are several exceptions for disclosing personally identifiable information without obtaining parental consent such as for sharing with School Official, including teachers within the same educational institution, or for Third-Party Research as described in the Data De-identified section, or with law enforcement. Applications and services are not required to disclose exceptions to obtaining parental consent under FERPA, if they do not engage in those practices. The difference in percentage of applications and services that disclose they engage in practices defined as COPPA exceptions (15%), could be because companies don't expose or share directory information as covered under a FERPA exception (7%).[293]

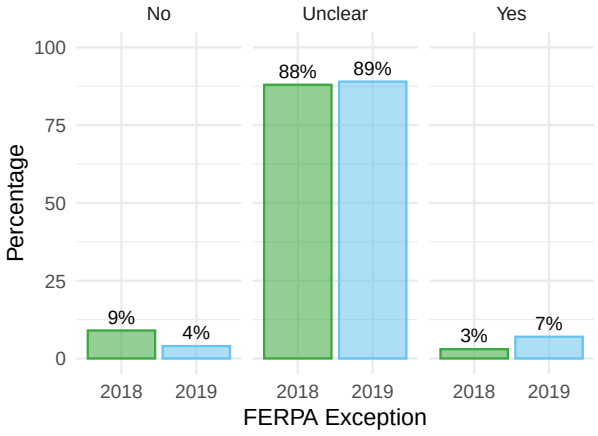


Figure 130: Do the policies clearly indicate whether or not the vendor may disclose personal information without verifiable parental consent under a FERPA exception?

Compared to 2018, applications and services evaluated in 2019 indicate a 4% increase in practices that companies may

[293] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.31(a)(1)(i)(A)-(B), 99.31(a)(3), 99.31(a)(6), 99.31(b)(1)-(2).

disclose personal information from students without verifiable parental consent under a FERPA exception. In addition, since 2018 there has been a trivial change in unclear practices. This small positive shift from qualitatively worse to qualitatively better practices may be the result of companies updating their policies to clarify they may contract with educational institutions as described in the School Contract section, or further clarify they may serve as a School Official, or disclose student data for Third-Party Research, or use for other purposes, as described in the Data Deidentified section, or are already obtaining verifiable Parental Consent prior to disclosing personal information

Directory Information

Among the applications and services we evaluated, approximately 2% indicated a qualitatively better response that they do not disclose "Directory Information" from students without verifiable parental consent under a FERPA exception. However, our analysis indicates a significant percentage, approximately 95% of applications and services evaluated, are unclear on this issue. In addition, our analysis indicates approximately 3% of applications and services evaluated indicated a qualitatively worse response that they do disclose "Directory Information" from students without verifiable parental consent under a FERPA exception.

Directory information is part of a student's education record, and includes personal information about a student that can be made public according to a school system's student records policy. In addition, directory information may include a student's name, home address, telephone number, and other information typically found in a school yearbook or athletic program. Each year schools must give parents notice of the types of information designated as directory information and the opportunity to provide opt-out consent.[294] Similarly to the FERPA Exception section, such a significant percentage of applications and services likely have unclear practices because they do not disclose "Directory Information" or believe sharing student directory information is an authorized exception under FERPA and they do not need to disclose their compliance obligations for exceptions in their policies.

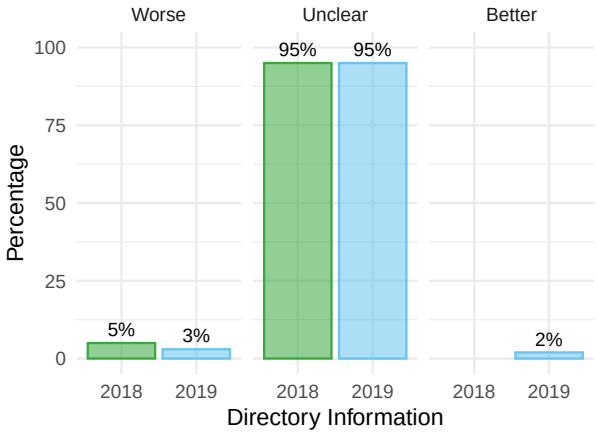


Figure 131: Do the policies clearly indicate whether or not the vendor discloses student information as 'Directory Information' under a FERPA exception?

Compared to 2018, applications and services evaluated in 2019 indicate no change in qualitatively better or worse practices that schools disclose student information as "Directory Information" under a FERPA exception. As described in the School Purpose and Students Intended sections, approximately 66% and 71% respectively disclose that the applications or services are intended for students and primarily designed, marketed, and for preschool or K-12 school purposes. Therefore, applications and services need to provide greater transparency on this issue, because these products are among the 150 most popular educational technology products, and there is a significant percentage of applications and services that disclose they are intended for children and students, but do not also disclose whether or not student information may be disclosed as "Directory Information" under a FERPA exception. 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.

[294] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.3; 99.37.

CONCLUSION

What is the state of edtech privacy in 2019? Since 2018, the state of edtech privacy has improved with overall privacy evaluation median Full Scores increasing by approximately 15%, from 45% to 52%. Additionally since last year, we have seen some significant improvements in the education technology industry across a wide range of privacy, security, safety, and compliance concerns. However, this improvement may still not be sufficient to protect kids using edtech products. Our findings in 2019 indicate a continuing widespread lack of transparency and inconsistent adoption of privacy and security practices across the industry for products intended for children and students.

Where did we see improvement? In a nutshell, there's been a lot of good news, covered in more detail in the Key Findings. A big improvement was the median Data Safety Scores, which saw a year-over-year increase of 45%, from 22% to 40% so we know that there are more transparent and qualitatively better practices related to promoting responsible use of data from children and students. Also, the median Ads & Tracking Scores saw a year-over-year increase of 37%, from 40% to 55%, illustrating more transparent and qualitatively better practices related to prohibiting the exploitation of users' decision-making process. We were also pleased to see that the median Data Rights Scores saw a year-over-year increase of 25%, from 60% to 75%, indicating that there were more transparent and qualitatively better practices related to users controlling data use. However, despite these areas where we saw improvement, there is still considerable room for additional progress.

Several concerns showed moderate improvement. The median Data Sold Scores saw a year-over-year increase of 16%, from 30% to 35%, indicating more transparent and qualitatively better practices related to preventing the sale of data. Likewise, the median Parental Consent Scores saw a year-over-year increase of 15%, from 52% to 60%, so we have some indication that the vendors are exhibiting more transparent and qualitatively better practices related to protecting children's personal information. The median Data Collection Scores saw a year-over-year increase of 12%, from 40% to 45%, indicating more transparent and qualitatively better practices related to protecting personal information. Similarly, the median Data Security Scores saw a year-over-year increase of 25%, from 40% to 50%, which includes a demonstrated interest in more transparent and qualitatively better practices related to protecting against unauthorized access. Still significantly, the median School Purpose Scores saw a year-over-year increase of approximately 11%, from 45% to 50%, so we were pleased that this indicates more transparent and qualitatively better practices related to following student data privacy laws. However, some things stayed the same, or roughly the same. The median Data Sharing Scores showed no change, showing that generally, companies did not update their policies in 2019 to disclose more transparent or qualitatively better practices related to protecting data from third parties.

In addition to the top 10 key findings, since 2018 many of the tier criteria questions used in the Evaluation Tiers indicated an increase in transparency, but disclosed both better and worse practices. Our Tier Key Findings indicate companies are slowly moving away from direct monetization and advertising using users' personal information, but they appear to be moving towards indirect advertising and monetization through third-party tracking. Still, overall we are encouraged that our research will continue to illuminate these practices and we will see steady year-over-year improvement in some of the positive trends we saw since 2018.

Given that 2018 was an extraordinary year for privacy, we had expected to see dramatic changes in the industry. Quite a lot happened to make 2018 a standout year in privacy. Our evaluation process was able to capture the state of edtech privacy before and after the most monumental shift in changes to privacy policies in the last decade, which accelerated dramatically in 2018. Specifically, we anticipated increased attention by vendors to privacy practices due to the new international focus on privacy protections from the GDPR and requirements flowing down to U.S. companies engaging in international business. We also noted the passage of laws in U.S. states, such as California's CCPA, the principles of which have inspired other state legislatures to take action. We've followed the impact of corporate privacy scandals that have thrown Facebook and Cambridge Analytica into the news and have generated public opinions on online privacy issues where no opinions or even comprehension existed previously. Finally, and this is not a new one, sadly, data breaches and other security incidents have continued to plague the edtech industry as they have other industries. Each time a customer receives a notice of data breach or suspected data breach in the mail, they realize how vulnerable their online data is to unauthorized access and use. With our research, we hope to raise all of these privacy issues, and, in addition, to highlight not just the possibility of unauthorized use, but also to raise awareness of the risks and harms associated with the collection, sharing, and use of child and student data in particular.

We observe changes in privacy policies of education technology and we analyze those changes in the aggregate for two important reasons. First, we note that change is possible. Too often, the media coverage around online privacy strikes a note of futility. "We can't change the system," they say. Economic pundits surmise that our entire economic system is built on an exchange of privacy for free services, and, in many cases, for paid services as well. Second, we note that

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

change is ongoing. Improvements in privacy awareness and privacy disclosures, which we expect to operate in a feedback loop going forward, will continue to result in year-over-year increases in our findings. How can we be so optimistic? While the degree of regulation of privacy disclosures may ebb and flow (although we strive to move these towards increased transparency as well), fundamentally once the public is aware of their rights, they are especially reluctant to forfeit them. Once a consumer thinks they are entitled to know what happens to their personal data once they input their information into the little boxes in an online form, it should be difficult to persuade them that they no longer have this right. Once a vendor has seen its customers flee in droves after the vendor has improperly used customer data entrusted to it, the vendor should be wary of another such breach of trust.

Still, we need this type of report and in-depth analysis of privacy practices in the edtech industry. The granularity of our research is critically important for impacting meaningful change. We intend to establish a comprehensive edtech privacy industry standard, composed of many laws, regulations, and best practices, that can be held up when someone asks: Why do we have to do this practice? What are the components of a good privacy policy? And more importantly, how do we effectuate good privacy practices? The answer is, look here, we have the state of edtech privacy report in hand and it says this is what our competitors are doing and what privacy protections our customers expect. This is the law. These are the best practices. This is the right thing to do to earn the respect of parents and educators.

With all of the privacy policy changes that have occurred in 2018, we suspect that many companies may be done making substantial privacy policy changes for the next year or two. That said, some companies are likely to be playing catch-up and others will be striving to ensure parents and teachers know they are privacy-focused, especially as privacy-related news scandals continue to create headlines. With that aim in mind, we hope that the suggestions made in this report, the incremental changes since last year in our evaluation process, as well as the comprehensive industry standards we apply in our evaluations, will encourage improvements in privacy practices and disclosures in vendors' privacy policy and terms of use even beyond the impact of a new law or publicized fines. We encourage vendors to use this report to implement privacy by design and security by design as part of their product-development and product-improvement processes. We will continue to educate parents about which details they should focus on and which practices warrant more scrutiny when determining what products are appropriate for their own children, both in terms of advocating for their children within the education system and for home use when appropriate.

A special note for policymakers: This report is full of valuable data to support your legislative initiatives. We know you want to protect children and students; in fact, many of you have made this your mission as part of your service to your school, state, or country. The findings we offer in this report are statistics of the state of privacy in the edtech industry to help build the scaffolding around future laws and regulations that go beyond assuming that an app that appeals to children is concerned with children's privacy. The conclusions we have drawn in this report can support your efforts to make the online marketplace safer for children and to retain the educational mission of our schools.

And a final message for educators: We're in this with you! Please let us know how we can help you support our children. The research summarized in this report started with educators' needs, and ends with this goal as well. We believe in the future of education, and this future starts with making sure that educators have what they need to make the classroom a place where magic happens.

APPENDIX

Transfer Data: Transfer Notice, Collection Limitation, Contractual Limits (pre-filter with mitigation techniques)

Of those 121 applications and services that indicated they allow the onward Transfer of Data (worse) highlighted blue in the event of a bankruptcy, acquisition, or merger, approximately only 20% are engaging in the following three mitigating practices. For these applications and services, it is critical that additional protections and mitigating practices be put in place to ensure that data cannot be used for a purpose other than the one it was originally collected for. Please see the respective sections for more details and analysis of the concerns Transfer Data, Transfer Notice, Collection Limitation, and Contractual Limits.

Table 24: Comparison of those 121 products that allow the Transfer Data with mitigating practices. Percentages are colored based on the number of mitigating practices used as follows: all three mitigating factors are indicated with blue, only two mitigating factors are colored orange and one or no mitigating factors are indicated with red.

Transfer Notice	Collection Limitation	Contractual Limits	Percent
Worse	Unclear	Unclear	1%
Worse	Better	Unclear	1%
Worse	Better	Better	2%
Unclear	Worse	Unclear	3%
Unclear	Worse	Better	1%
Unclear	Unclear	Unclear	12%
Unclear	Unclear	Better	10%
Unclear	Better	Unclear	19%
Unclear	Better	Better	18%
Better	Worse	Unclear	1%
Better	Worse	Better	1%
Better	Unclear	Worse	1%
Better	Unclear	Better	2%
Better	Better	Worse	1%
Better	Better	Unclear	8%
Better	Better	Better	20%

Unsafe Interactions and Share Profile (comparison)

Of those 42% of applications and services allowing Unsafe Interactions (worse) highlighted gray, it is critical that additional protections and mitigating practices be put in place to allow unsafe interactions without also sharing profile information. Unfortunately, we see that approximately 12% (5/42) of that 42% mitigates this practice by not requiring users to share profile information. Please see the respective sections for more details and analysis of the concerns Unsafe Interactions and Share Profile.

Table 25: Unsafe interactions and Share Profile. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Unsafe Interactions	Share Profile	Percent
Worse	Worse	28%
Worse	Unclear	9%
Worse	Better	5%
Unclear	Worse	6%
Unclear	Unclear	31%
Unclear	Better	2%
Better	Worse	11%
Better	Unclear	2%
Better	Better	6%

Visible Data and Control Visibility (comparison)

Of those 47% of applications and services allowing Visible Data (worse) highlighted gray, it is critical that additional protections and mitigating practices be put in place to allow users to control the visibility of their information with the default visibility of data being the most restrictive. We see that approximately 81% (38/47) of that 47% mitigates this practice by providing privacy controls to limit visibility of data that can be made publicly available. Please see the respective sections for more details and analysis of the concerns Visible Data and Control Visibility.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Table 26: Visible Data and Control Visibility. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Visible Data	Control Visibility	Percent
Worse	Worse	2%
Worse	Unclear	7%
Worse	Better	38%
Unclear	Unclear	30%
Unclear	Better	3%
Better	Worse	1%
Better	Unclear	7%
Better	Better	11%

Children Intended: Moderating Interactions (pre-filter with mitigation technique)

Of those 102 applications and services that disclose children are intended, it is critical that additional protections and mitigating practices be put in place to moderate interactions to protect children from potential social, emotional, or physical harm. Unfortunately, we see that only 14% of the industry is engaging in the following mitigating practice of moderating safe or unsafe interactions with products intended for children. Please see the respective sections for more details and analysis of the concerns Children Intended and Moderating Interactions.

Table 27: Of those 102 applications or services that indicated children are intended, which engage in the practices of Moderating Interactions.

Moderating Interactions	Percent
Worse	23%
Unclear	64%
Better	14%

Traditional Ads and Unsubscribe Ads (comparison)

Of those 47% of applications and services with Traditional Ads (worse) highlighted gray, it is critical that additional protections and mitigating practices be put in place to allow users to unsubscribe from advertisements. We see that approximately 67% (31/47) of that 47% mitigates this practice by allowing users to unsubscribe from advertisements. Please see the respective sections for more details and analysis of the concerns Traditional Ads and Unsubscribe Ads.

Table 28: Traditional Ads and Unsubscribe Ads. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Traditional Ads	Unsubscribe Ads	Percent
Worse	Worse	1%
Worse	Unclear	15%
Worse	Better	31%
Unclear	Worse	1%
Unclear	Unclear	28%
Unclear	Better	1%
Better	Worse	2%
Better	Unclear	17%
Better	Better	5%

Behavioral Ads and Unsubscribe Ads (comparison)

Of those 33% of applications and services with Behavioral Ads (worse) highlighted gray, it is critical that additional protections and mitigating practices be put in place to allow users to unsubscribe from advertisements. We see that approximately 58% (19/33) of that 33% mitigates this practice by allowing users to unsubscribe from advertisements. Please see the respective sections for more details and analysis of the concerns Behavioral Ads and Unsubscribe Ads.

Table 29: Behavioral Ads and Unsubscribe Ads. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Behavioral Ads	Unsubscribe Ads	Percent
Worse	Worse	3%
Worse	Unclear	11%
Worse	Better	19%
Unclear	Unclear	19%
Unclear	Better	2%
Better	Worse	1%
Better	Unclear	29%
Better	Better	15%

Third-Party Marketing and Unsubscribe Marketing (comparison)

Of those 32% of applications and services with Third-Party Marketing (worse), highlighted gray, it is critical that additional protections and mitigating practices be put in place to allow users to unsubscribe from marketing communications. We see that approximately 84% (27/32) of that 32% of the industry mitigating that practice by allowing users to unsubscribe from marketing. Please see the respective sections for more details and analysis of the concerns Third-Party Marketing and Unsubscribe Marketing.

Table 30: Third-Party Marketing and Unsubscribe Marketing. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Third-Party Marketing	Unsubscribe Marketing	Percent
Worse	Worse	1%
Worse	Unclear	4%
Worse	Better	27%
Unclear	Unclear	10%
Unclear	Better	11%
Better	Unclear	18%
Better	Better	29%

Marketing Messages and Unsubscribe Marketing (comparison)

Of those 71% of applications and services with Marketing Messages (worse) highlighted gray, it is critical that additional protections and mitigating practices be put in place to allow users to unsubscribe from marketing communications. We see that approximately 83% (59/71) of those 71% mitigating this practice by allowing users to unsubscribe from marketing. Please see the respective sections for more details and analysis of the concerns Marketing Messages and Unsubscribe Marketing.

Table 31: Marketing Messages and Unsubscribe Marketing. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Marketing Messages	Unsubscribe Marketing	Percent
Worse	Worse	1%
Worse	Unclear	11%
Worse	Better	59%
Unclear	Worse	1%
Unclear	Unclear	19%
Unclear	Better	6%
Better	Unclear	3%
Better	Better	1%

Children Intended & Parental Consent: Consent Method, COPPA Notice (multiple pre-filter with mitigation techniques)

Of those 92 applications and services that indicate children are intended and also obtain parental consent before they collect or disclose personal information from children, the following mitigating practices are in place with respect to the Consent Method and COPPA Notice concerns highlighted in blue. We see that 59% of the industry is engaging in the following mitigating practices of disclosing the method of providing parental consent and including additional details of how COPPA applies to protecting information collected from children under 13 years of age which allows parents to provide informed consent.

Table 32: Of those 92 applications and services indicating that children are Intended and Parental Consent is obtained prior to collecting or disclosing personal information review Consent Method and COPPA Notice. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Consent Method	COPPA Notice	Percent
Worse	Better	1%
Unclear	Unclear	5%
Unclear	Better	29%
Better	Unclear	5%
Better	Better	59%

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Data Shared: Combination Limits and Data Deidentified (pre-filter with mitigation techniques)

Of those 144 applications and services that indicate data is shared with third parties, the following mitigating practices are in place with respect to the Combination Limits and Data Deidentified concerns. We see that 11% of the industry is engaging in the following mitigating practice of requiring combination limits on third parties to prevent any re-identification of any data shared with them and sharing data with third parties in an anonymized or deidentified format. Without placing combination limits on data that is shared with third parties, the majority of practices intended to protect data are rendered useless or less effective. It is absolutely critical, especially given the power of big data, that combination limits be placed on all data that is shared with third parties. Unfortunately, we only see 13% of applications and services indicate that when data is shared they also appropriately place limits on recombination of that data.

Table 33: Of those 144 applications and services indicating that data is shared review Combination Limits and Data Deidentified. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Combination Limits	Data Deidentified	Percent
Worse	No	1%
Worse	Yes	1%
Unclear	No	15%
Unclear	Unclear	26%
Unclear	Yes	44%
Better	No	1%
Better	Unclear	1%
Better	Yes	11%

Withdraw Consent: Retention Policy and Delete Child PII (pre-filter with mitigation techniques)

Of those 71 applications and services that indicated they allow parents to withdraw consent, we see that only 49% clarify what their retention policy is, and disclose they delete personal information from a student or child under 13 years of age if collected without parental consent. We would expect more applications and services to clarify that they delete personal information if collected without parental consent from kids under 13. The complexity of the real world indicates that inadvertent or unintentional collection of personal information from kids under 13 may occur, even if an application or service intends to only collect personal information from kids under 13 after parental consent is obtained. As such, policies should be clear that the application or service will appropriately delete any data collected without appropriate parental consent.

Table 34: Of those 71 applications and services indicating they allow parents to withdraw consent, which engage in the practices of Retention Policy and Delete Child PII.

Retention Policy	Delete Child PII	Percent
No	Unclear	10%
Yes	Worse	1%
Yes	Unclear	39%
Yes	Better	49%

Children or Students Intended Parental Consent: Delete Child PII (multiple pre-filter with mitigation technique)

Of those 100 applications indicating that either children or students are intended and indicate that parental consent is obtained before collecting or disclosing personal information, we see that 64% have clarified they will delete personal information if collected without parental consent from kids under 13. The complexity of the real world indicates that inadvertent or unintentional collection of personal information from kids under 13 may occur. As such, policies should be clear that the application or service will appropriately delete any data collected without appropriate parental consent.

Table 35: Of those 100 applications and services where parental consent is obtained before they collect or disclose personal information, what are the practices where children or students are intended relative to the practice of Delete Child PII.

Delete Child PII	Percent
Worse	1%
Unclear	35%
Better	64%

Children or Students Intended & Parental Consent: Consent Method (multiple pre-filter with mitigation technique)

Of those 100 applications indicating that either children or students are intended and indicate that parental consent is obtained before collecting or disclosing personal information, we see that 60% clarify the method used to obtain parental consent. We would expect this to be 100%, because this subset is from applications and services that understand parental consent is necessary, but are not clarifying how parents should actually provide verifiable consent.

Table 36: Of those 100 applications and services where parental consent is obtained before they collect or disclose personal information, what are the practices where children or students are intended relative to the practice of Consent Method.

Consent Method	Percent
Worse	1%
Unclear	39%
Better	60%

School Purpose: Students Intended and Teachers Intended (pre-filter with multiple mitigation techniques)

Of those 51 applications and services that are either unclear or indicate they are not primarily used, designed, and marketed for preK-12 or are unclear table 37 examines the combination of responses to whether or not teachers are intended, whether or not students are intendedIt is assumed these are general audience applications, yet still used in an educational setting. If an application or service is not primarily designed for preK-12 purposes. PreK-12 districts and teachers should exercise additional caution to understand what types of other users will be using the application as well as determining whether or not additional safety procedures, contract addendums, and additional configuration is necessary in order to use the application or services as safely as possible.

Table 37: Comparison of those 51 applications and services that are unclear whether or not or indicate the product was not primarily designed for preK-12 compare students and teachers intended.

Students Intended	Teachers Intended	Percent
No	Yes	4%
Unclear	Unclear	69%
Unclear	Yes	4%
Yes	Unclear	8%
Yes	Yes	16%

Students Intended: Student Data and Education Records (pre-filter with mitigation techniques)

Of those 107 applications and services that indicate they are intended for students it is critical that companies disclose the collection of personal information or education records from preK-12 students, and the process by which education records are entered into the product. Fortunately, we see 77% are clarifying how education records are entered into the product. Of the remaining percentage of applications and services, we would like to see those additional 9% that indicate they do collect student data clarifying how data is entered into the system.

Table 38: Of those 107 applications and services indicating that students intended review Student Data and Education Records.

Student Data	Education Records	Percent
Worse	No	9%
Worse	Yes	72%
Unclear	No	11%
Unclear	Yes	4%
Better	No	3%
Better	Yes	1%

School Contract: School Official versus School Consent (pre-filter with mitigation techniques)

Of those 56 applications and services that indicate they provide a contract to a Local Educational Agency (LEA) or otherwise provide notice to users of additional rights, it is crit-

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

ical that companies disclose whether or not the vendor is under the direct control of the educational institution and designates themselves a School Official under FERPA, and whether or not responsibility or liability for obtaining verifiable parental consent is transferred to the school or district (School Consent). Unfortunately, we see 80% of applications and services are transferring responsibility or liability for obtaining parental consent to the school or district, which may be because if a company agrees to provide additional protections in a contract, the company assumes that contract will disclose the verifiable parental consent obligations of both parties. However, schools and districts still need to understand what those specific additional protections should be in the policies, and then begin a lengthy negotiation process where gaps in protecting student data have been identified.

Table 39: Of those 56 applications and services indicating a contract to a Local Educational Agency (LEA) or otherwise provides notice to users of additional rights review School Official and School Consent. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

School Official	School Consent	Percent
Worse	Worse	4%
Unclear	Worse	29%
Unclear	Unclear	11%
Unclear	Better	2%
Better	Worse	48%
Better	Unclear	7%

Safe or Unsafe Interactions: Log Interactions versus Moderating Interactions (pre-filter with mitigation techniques)

Of those 91 applications and services that indicate Safe Interactions or Unsafe Interactions are available it is critical that additional protections and mitigating practices be put in place to log and moderate social interactions between users and make them available for review or audit. Unfortunately, we only see 10% of applications and services both logging and moderating interactions which are necessary to ensure safe interactions between users are age appropriate. These protections are intended to prevent potential social, emotional, or physical harm as a result of harassment, stalking, and/or cyberbullying using these communication platforms, but must also be used by schools or districts in a responsible manner with students' full knowledge and consent.

Table 40: Of those 91 applications and services indicating either safe or unsafe interactions are allowed review the relation between Log Interactions and Moderating Interactions. Percentages are colored as follows: if both practices are Better they are colored blue, if only one practice is Better they are colored orange, and if no practices are Better they are colored red.

Log Interactions	Moderating Interactions	Percent
Worse	Worse	1%
Unclear	Worse	21%
Unclear	Unclear	46%
Unclear	Better	11%
Better	Worse	1%
Better	Unclear	10%
Better	Better	10%

Parental Consent, Data Shared, Advertising & Marketing: Limit Consent (pre-filter with mitigation technique)

Of those 65 applications and services that indicate parental consent is obtained before they collect or share personal information, and either use traditional advertising, behavioral advertising, or engage in third-party marketing, can parents provide consent but limit their consent to the collection of their child's personal information without also consenting to the disclosure of that information to third parties. We see that only 20% allow parents to provide consent to the collection and use of their child's personal information and allow it to be limited to exclude third-party use in an advertising or marketing context. Additionally, a large majority of applications and services are unclear on this practice. We expect companies to provide more information to parents to allow them to provide informed consent and limit the use of their child's personal information to first-party intended use.

Table 41: Of those 65 applications and services that share data and provide any marketing or advertising, but allow parental consent to be limited to only first-party intended use.

Limit Consent	Percent
Worse	3%
Unclear	77%
Better	20%

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

© 2019 Common Sense Media. All rights reserved.
Common Sense, associated names, associated trademarks, and logos are trademarks of Common Sense Media, a 501(c)(3) nonprofit organization, FEIN 41-2024986.