2021

STATE OF KIDS' PRIVACY

common sense®

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

CREDITS

Authors:	Girard Kelly, Common Sense Media Jeff Graham, Common Sense Media Jill Bronfman, Common Sense Media Steve Garton, Common Sense Media
Contributors:	Johanna Gunawan Taylor Deitrick
Data analysis:	Girard Kelly, Common Sense Media Jeff Graham, Common Sense Media
Copy editor:	Tasha Kelter
Designer:	Jeff Graham, Common Sense Media

Suggested citation: Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). *2021 State of Kids' Privacy*. San Francisco, CA: Common Sense Media

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The *2021 State of Kids' Privacy* report represents the culmination of our research over the past five years in evaluating hundreds of education and consumer technology-related applications and services. Our evaluations include a careful reading and in-depth analysis of all the publicly available privacy policies and terms of use by trained privacy attorneys and privacy experts in order to rate and score products with the highest possible quality and accuracy on a 100-point scale across 155 unique evaluation questions. This report includes our findings from evaluations of 200 products' privacy policies in 2020 and 2021 from the most popular kids tech and edtech applications and services, as determined from interviews with various parents, teachers, schools, and districts, as well as total Apple and Google App Store downloads during the past 12 months in the kids and education categories. While we started evaluating apps in 2018 that might be used primarily by children under 13 years old and students in pre-K through 12th grade, our privacy evaluation process has since expanded to also examine the privacy practices of products for teens and adult consumers. In addition, products added since 2020 include more child-intended products rather than only student-intended products in order to create a more diverse and representative sample of the real-world environment in which children use tech products both at home and in the classroom. The 2021 data in this report is compared to our findings over the past four years to provide a detailed look back at the privacy practices in the industry over time with a focus on kids.

Consumers' expectations of privacy have changed dramatically over the past few years with the passage of new state privacy laws across the nation. Companies have since adapted and changed their privacy practices in response. This monumental shift in focus and attention on the privacy practices of companies' products is also the result of a changing privacy compliance landscape. Legislative initiatives such as the European-based General Data Protection Regulation (GDPR) in 2018, and the corresponding California Consumer Privacy Act (CCPA) in 2019, as well as the passage of several other state privacy laws across the nation including the California Privacy Rights Act (CPRA) in 2020, created a new narrative that highlighted the privacy shortcomings of big tech and social media companies, leading consumers to look more closely at the privacy practices of the products they use every day. These factors prompted companies to update their policies at an unprecedented rate. Over half of the most popular applications and services evaluated in this report have had to be completely re-evaluated every year due to legislative privacy changes and shifts in consumer expectations.

In 2020, as a result of the COVID-19 pandemic accelerating the already existing progress toward online education, we have added new products, as well as removed discontinued and lesser-used products. The 200 products used in this report are a snapshot and moving target of what we know from parents and educators to be the most popular applications and services used in the classroom by students and children at home in 2021. The privacy evaluations used in this report are continually updated and available on our Common Sense Privacy Program website, and we encourage readers to utilize these free resources to supplement the reading of this report.

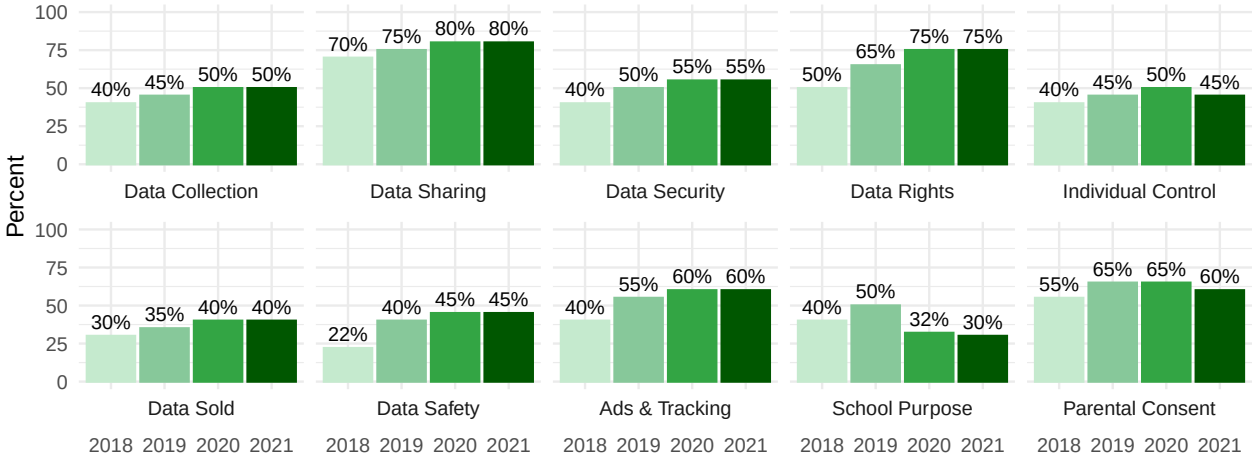
In 2021, the State of Kids' privacy is far below parents' expectations, and products used by children are not nearly as privacy-protecting as they should be.

Despite the rapid pace of change in the industry, many companies have not updated their policies with better privacy-protecting practices to keep pace with changes in legal requirements and privacy best practices. As a result, there is still a widespread lack of transparency across all our evaluation questions, as well as inconsistent practices that apply to some users but not others, and "unclear" practices for both kids' tech and edtech applications and services directed toward children and students. However, the good news is that the overall full evaluation median scores have incrementally increased year-over-year since 2018 by 20%, and the majority of the evaluation concern category median scores are stable in 2020.

The following chart summarizes our Evaluation Concerns category median scores:

While these stable median scores are somewhat promising for transparency, there is still considerable work that needs to be done. The majority of applications and services analyzed in this report used by children or students either do not adequately define safeguards taken to protect child or student information, or they lack

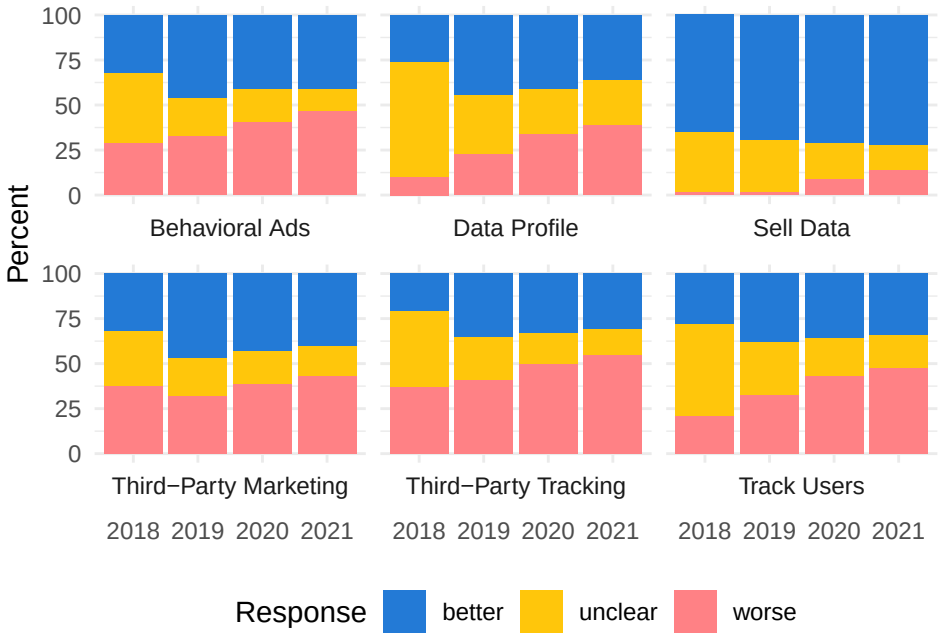
Figure 1: Key findings indicating median score changes year-over-year results



a detailed privacy policy. While the number of products that meet our minimum safeguards that protect all users of a product, and therefore receive a Pass rating, more than doubled since 2018 from 10% to 26%, that still leaves 74% of applications and services in 2021 with our Warning rating that means they are not meeting our minimum privacy recommendation threshold. As privacy laws continue to be passed that focus on more of the privacy practices used in our *Warning* rating, applications and services with a *Warning* rating are more likely to change their privacy practices next year to keep pace with changing compliance obligations or risk falling further behind the industry.

The following chart summarizes the percentages of "better," "unclear," or "worse" responses to evaluation questions used in our Evaluation Ratings:

Figure 2: Key findings indicating changes in responses to rating-related questions year-over-year results



Technology platforms used by children and students serve an especially vulnerable population and should be held accountable and to a higher standard. The lack of transparency, as shown in figure 2's "unclear" responses and 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 already transparent in their policies

about their privacy practices also tend to engage in qualitatively "better" privacy and security practices. However, our analysis also indicates that products that are not transparent are typically withholding "worse" practices, especially practices that involve a product's monetization of its users' data. Yet when practices are not disclosed, there can be no standard of trust from parents, teachers, schools, or districts about how information collected from children and students will be handled and protected. 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, children, and parents.

There has also been improvement with a small number of companies updating their policies with "better" privacy practices to differentiate their products from the rest of the industry. These companies use our ratings and evaluation questions to better communicate to their users how they respect privacy. Further, they are trying to set an example for the entire industry by showing that privacy can be a competitive advantage in the marketplace for parents and educators who are looking for products with "better" privacy-protecting practices for themselves and their children and students.

Unfortunately, there is still far too little attention paid to the privacy and security practices of technology platforms that affect tens of millions of children on a daily basis. It is vital that educators, parents, and policymakers engage in an open dialogue with companies to build solutions that strengthen our children's privacy and security protections. This report can inform those critical conversations, and we intend to continue our research with biannual updates and resources for policy makers on the evolving State of Kids' 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 300 schools and districts, we are working in collaboration with third-party software developers of products we evaluated 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 first *State of EdTech Report* was published in 2018.[1] We have spoken with numerous teachers, students, parents, developers, companies, privacy advocates, and industry representatives about their perspectives on privacy to inform our work.

The *2021 State of Kids' Privacy* report represents the culmination of our research over the past five years in evaluating hundreds of education technology-related applications and services. The report includes findings from evaluations of 200 products' privacy policies from the most popular edtech applications and services, as determined from interviews with various teachers, schools, and districts as well as total App Store downloads during the past 12 months in the kids and education categories. Our 2021 data is compared to our findings over the past four years to provide a detailed look back at the privacy practices in the industry over time. In addition, due to our increase in the number of products evaluated each year from 2018 to 2020 and the product demographic shift from primarily edtech prior to 2020 to also include kids' tech in 2020 and beyond, we also considered the sub-population of products evaluated across all four years in every aspect of the report, and where we saw any differing trends we call them out specifically. The applications and services evaluated for this report provide a representative sample of the most popular kids tech and educational technologies that include educational games and tools for communication, collaboration, formative assessment, student feedback, content creation, and delivery of instructional content. Child-directed applications and services that are used at home by kids, including games, apps for communication, collaboration, content creation, and media entertainment, were also evaluated. The applications and services evaluated 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.

The State of Kids' Privacy has been directly impacted by consumer privacy laws that were passed in 2018 and included 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) in 2019 and subsequent California Privacy Rights Act (CPRA) in 2020 that provides consumers with the right to opt out of the sale of their personal information to third parties.[2,3] Privacy policy changes that began in 2018 continued and accelerated in the following years due to the passage of the CCPA, its successor the CPRA, and a host of other state-specific consumer privacy laws that were introduced in state legislatures around the country that put increased pressure on companies to follow the GDPR, California's privacy law, its promulgated regulations, and similar consumer privacy legislation in other states.[4] As a result, the privacy policies we examined changed in waves, with the crest of some of these waves identifiable in the timeline to take effect exactly on the date when each of these new laws and regulations took effect. In many cases, policy edits closely followed the letter of the new laws, with increases in transparency resulting in the disclosure of "worse" practices. Some companies even quoted the language of new laws and attempted to interpret the language right in the privacy policy, with many companies in 2019 and 2020 disclosing they are not quite sure if they "sell" users' data to third parties, as defined under the CCPA.

While we closely examine new statutes and regulations and assign points for transparency with the requirements outlined in the regulations, we also seek to establish best practices for the implementation of these laws. As a consequence, we are keenly

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

[3] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.100-1798.198.

[4] International Association of Privacy Professionals (IAPP), *US State Privacy Legislation Tracker*, https://iapp.org/resources/article/us-state-privacy-legislation-tracker.

attuned to the small differences in wording of the privacy policy provisions that either specifically limit the promises of new rights and abilities to a particular jurisdiction or type of user versus those that expand the application of the new laws to all users. In some cases it may be appropriate to limit privacy protections to children under the age of 13, such as for parental permissions. However, it is almost never ethically defensible to limit a privacy-protective provision to just someone in the state of California, while denying such protection to someone in a neighboring state. Many companies may look at their own logistics and operational costs and discover it is easier and less expensive for their company[5] to offer privacy protections to all users, due to economies of scale and the transactional costs of compliance. Our evaluation process awards the most points for transparency and "better" practices to policies that grant privacy protections to all users, regardless of the jurisdictional legal obligation.

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 150 privacy- and security-related questions[6] that are expected to be disclosed in policies for products used in an educational or consumer context. In addition, both qualitative and quantitative methods were developed, as described in our Methodology section, to determine both the particular issues companies disclose in their policies and the meaning behind those disclosures. As a result, the Common Sense Privacy Program has produced a substantial body of work, including these crucial privacy evaluations available to the public for review, analysis, and consumer education. The report covers only a small portion of the conclusions that could be drawn from the rich data created by these evaluations. Looking at the privacy policies and terms of service for the top 200 educational and consumer apps used by children and students is a great place to start illuminating the dark corners of the industry and increasing the standards for kids' privacy.

[5]The term "company" in this report is used generally to refer to edtech "vendors," mobile "developers," and "operators" of applications or services.

[6]Common Sense Media, *Full Evaluation Questions*, Privacy Program, https://github.com/commonsense-org/privacy-questions-output/blob/main/full-questions.md.

The Common Sense Privacy Program was created to champion child and student privacy and support parents, educators, schools, and policymakers on a path toward a more secure and safe future for all kids.

Parents and educators can use our easy-to-understand privacy evaluations to make informed choices about the products they use with children at home and with students in the classroom. Our evaluation summaries show how companies address safety, security, privacy, and compliance in their policies and terms of service. Privacy evaluations help educators decide which tools to use with students in the classroom and in their daily lives in a more informed and efficient manner.

We acknowledge the equity issues inherent in our evaluation processes. Our privacy evaluations attempt to level the playing field to allow any consumer, parent, educator, child, or student to understand a product's baseline privacy practices of the product for free. We hope this encourages companies to improve their baseline privacy practices that apply to all users of the product so that custom-negotiated contracts used to increase a user's privacy protections are less necessary. However, large school districts and other educational entities with more resources may negotiate better privacy-protective terms and additional services with specific companies. These contracts supplement and in some cases supersede the policies and terms in the publicly available policies that we use for our evaluations.[7] However, parents and guardians are not all similarly situated with regard to educational and economic resources or the ability to negotiate better privacy-protecting terms with a company. When parents interact with the privacy policies we evaluate, some may not be able to take advantage of the additional privacy-protective options offered by the privacy policies due to a lack of language options, or reading ability, or time. Nevertheless, we offer our evaluations in the context of illuminating the process for everyone.

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 applications and services they use. We believe that companies and software developers can

[7]*See* Student Data Privacy Consortium (SDPC), https://privacy.a4l.org.

make better and safer products for children and students with this knowledge. We hope this data will help show the potential impact that privacy and security practices have on the lives of millions of children and students who use technology every day and help support meaningful and positive changes. The following 2021 report illustrates our methodologies, results, categorical concerns, and key findings of privacy and security practices used by 200 popular kids' tech and edtech applications and services. Please see the appendix Product Population Demographics for a breakdown of our product populations.

Guidelines: A special note on how to use this report

- For **policymakers and regulators**: This report is full of 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. The findings in this report should serve as a wake-up call that the state of kids' privacy is so poor that stronger privacy laws and enforcement are critically needed to better protect the privacy of our children and students. In addition, the findings in this report should also serve to provide regulators with the information they need to make better-informed decisions in order to pursue more focused and meaningful enforcement of products potentially violating federal or state privacy laws, or engaging in unfair or deceptive practices that may be unavoidable by children and students.
- For **consumers**: The top 200 applications and services examined in this report are products you likely use every day, but you may not be aware of the wide range of different privacy practices among them. The privacy concerns and issues we identify in the report can help you understand the areas to apply more scrutiny to when choosing products and services.
- 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. Individual product evaluations can help inform your decisions, but this report can also help highlight areas that you may not have been concerned about but probably should consider now given our findings of "worse" privacy practices across the industry. The results of this report may also inspire you to help support legislation that protects child and student privacy at the local, state, and federal levels.
- 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 to 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. This report can also help identify particular issues that may require supplemental student data privacy agreements with companies, or areas that warrant additional scrutiny for consumer apps used in classrooms.
- 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 analysis goes beyond summarizing existing industry practices to forecasting industry trends and establishing best practices going forward. 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 companies and users.
- For **companies and trade associations**: The overall findings in this report and our individual company privacy evaluations are both valuable tools to assess the state of the industry. We encourage companies 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 applications and services from the industry at large.

Key Findings

Our overall findings in 2021 indicate a widespread lack of transparency and inconsistent privacy and security practices that apply to some users, but not to others, for products intended for children and students. However, since 2018, the state of privacy has improved, with the median overall privacy evaluation full scores increasing year-over-year by approximately 20% from 41% to a median of 49%. Higher median scores are always better in our evaluation process, but the 2021 overall median full score is still lower than expected, given that these applications and services are intended for children and students. An increase since 2018 in privacy evaluation median full scores generally indicates more transparent and qualitatively "better" practices disclosed in companies' policies across a wide range of privacy, security, safety, and compliance concerns.

Note that disclosure of a risky practice by a company results in a "worse" label, whereas an "unclear" label indicates a company failed to disclose any details about that particular issue and as a result it is unclear whether the company's practice is "better" or "worse" for our evaluation purposes. The trend towards increasing *"worse"* labels is not entirely bad. Most of the increase in *"worse"* labels we see is the direct result of the decrease in *"unclear"* labels as a result of privacy policies generally becoming more transparent. We find this information empowering, even as the proportion of *"worse"* labels increases. Understanding a product's practices allows for more informed decisions by parents and educators, as well as better-informed legislators and regulators who can enact stronger legislation requiring better disclosures about issues, and more privacy protecting practices.

Our overall top-6 key findings are illustrative of current privacy and security trends in the kids' tech and edtech industry.

1. *Transparency continues to increase*.

Over the past four years, we have seen significant increases in transparency on almost every single full evaluation question. Companies' privacy policies are more comprehensive and transparent than they have ever been. This increase in transparency means a wider range of issues are addressed in a company's policy and not ignored, allowing consumers, parents, and educators to make better informed decisions and compare products on privacy practices. While general trends are towards improved transparency, companies need to do better to address their users' interests by being even more transparent in their policies, rather than just disclosing the minimum details for compliance. For some products there is already a high level of transparency across all details and concern categories indicating that our expectations for transparency are not unreasonable, but the industry still has considerable room for improvement.

2. *Full median scores are stable*.

The full evaluation median scores are relatively stable over the past two years. Therefore, the industry needs to step up and improve its transparency across a wide range of issues in order to increase the Full Score, which will mean there is more information available to make an informed decision on whether to use a product. However, we also need to look deeper at each evaluation question to see what, if any, changes are happening over the short term (past two years) and long term (past 4 years). For example, are minimum and maximum scores improving, or are there fewer outliers especially in the low score areas?

3. *Concern category details are shifting*.

The Concern Category scores (10 questions) are relatively stable over the past two years. The privacy evaluation process summarizes the policies of a product into concern categories based on a subset of evaluation questions that can be used to quickly identify particular strengths and weaknesses of a company's policies. However, when we take a deeper look at the evaluation questions within each category over the past two years, we have a mix of both positive and negative shifts depending on the question and despite stable concern category scores.

4. ***Rating practices are more transparent.***
Companies are updating their privacy policies more frequently to discuss the issues related to our Evaluation Ratings criteria. However, many companies that change their privacy policy to address a rating criteria issue, whether it is in response to new privacy legislation or pressure from consumers with increased awareness or expectations of privacy, unfortunately often disclose "worse" practices for kids and families. Despite this huge increase in transparency, many products are still non-transparent on two or more of our seven rating criteria, and provide a level of transparency considerably lower than the industry standard.

5. ***Evaluation question scores are stable.***
Many of the full evaluation questions have been relatively stable over the past two years. This indicates companies are not making significant recent changes to their privacy policies related to the issues identified in our evaluation question framework. We speculate that this may be due to the fact that the majority of legislative and compliance policy changes from the GDPR (2018) and CCPA (2019) are now accounted for, and we expect companies to update their policies again in 2022 in response to new consumer privacy legislation such as the CPRA's requirements and future federal privacy legislation.

6. ***Challenges to make informed decisions.***
Although transparency continues to increase across all of our evaluation questions, which is promising, transparency in privacy policies is still far too low, and policies are too long and too complicated. For those few who have the time to read and can understand the policies, there is not sufficient information available to adequately cover all the different privacy issues and contexts of how a product can be used. Without higher percentages of transparency in our basic questions and rating criteria questions, parents, educators, and consumers cannot realistically make informed decisions.

Concern Category Findings

Our findings also include changes across several issue areas of concern for consumers, parents, and educators in the long term since 2018. Concern categories are useful to highlight qualitative differences in privacy practices between products that can't be quantitatively assessed when aggregated with all the evaluation questions. Higher median concern category scores are always better in our evaluation process, but the 2021 concern median scores are still lower than expected, given that these applications and services are used by children and students. Our evaluation process includes the following concern categories: Data Collection, Data Sharing, Data Security, Data Rights, Individual Control, Data Sold, Data Safety, Ads and Tracking, Parental Consent, and School Purpose.

The top-10 concern category findings illustrate stable median scores across a wide range of issues:

1. *Since 2020 the* ***Data Collection*** *concern median score is stable at 50%.*
While the Data Collection median score saw an approximate increase of 25% from 2018 to 2020, indicating that applications and services increased transparency related to collecting personal information, we have seen no significant change after 2020.

2. *Since 2020 the* ***Data Sharing*** *concern median score is stable at 80%.*
While the Data Sharing median score saw an approximate increase of 14% from 2018 to 2020, indicating that applications and services increased transparency related to protecting data shared with third parties, we have seen no significant change after 2020.

3. *Since 2020 the* ***Data Security*** *concern median score is stable at 55%.*
While the Data Security median score saw an approximate increase of 38% from 2018 to 2020, indicating that applications and services increased transparency related to protecting against unauthorized access, we have seen no significant change after 2020.

4. *Since 2020 the **Data Rights** concern median score is stable at 75%.*

While the Data Rights median score saw an increase of 50% from 2018 to 2020, indicating that applications and services increased transparency related to controlling data use, we have seen no significant change after 2020.

5. *Since 2020 the **Individual Control** median score decreased to 45%.*

While the Individual Control median score saw an increase of approximately 13% from 2018 to 2020, indicating that applications and services increased transparency related to providing informed consent, we have seen a decrease of approximately 10% after 2020.

6. *Since 2020 the **Data Sold** concern median score is stable at 40%.*

While the Data Sold median score saw an increase of approximately 33% from 2018 to 2020, indicating that applications and services increased transparency related to the sale of data, we have seen no significant change after 2020.

7. *Since 2020 the **Data Safety** concern median score is stable at 45%.*

While the Data Safety median score saw an increase of approximately 105% from 2018 to 2020, indicating that applications and services increased transparency related to promoting responsible use, we have seen no significant change after 2020.

8. *Since 2020 the **Ads & Tracking** concern median score is stable at 60%.*

While the Ads & Tracking median score saw an increase of approximately 50% from 2018 to 2020, indicating that applications and services increased transparency related to targeted advertisements and tracking, we have seen no significant change after 2020.

9. *Since 2020 the **Parental Consent** concern median score decreased to 60%.*

While the Parental Consent median score saw an approximate increase of 18% from 2018 to 2020, indicating that applications and services increased transparency related to protecting children's personal information, we have seen a decrease of approximately 9% from 2020.

10. *Since 2020 the **School Purpose** concern median score is relatively stable at 30%.*

While the School Purpose median score saw an approximate decrease of 25% from 2018 to 2020, indicating that applications and services decreased transparency related to compliance with student data privacy laws, we have seen no significant change after 2020.

Rating Findings

The Evaluation Ratings are based on a handful of the most important issues related to selling data, targeted advertisements, and tracking users that are used by parents, educators, and consumers when determining whether to use a product. Our rating related question findings indicate a continued lack of transparency and an unfortunately high percentage of "worse" privacy practices for products intended for children and students. However, since 2018, many of the questions used in our evaluation ratings indicate a decrease in "unclear" responses, resulting in an increase in both "better" and "worse" practices. Please see our Evaluation Scores section for more details about our scoring methodology.

Our findings look at evaluation rating criteria and related evaluation questions that include: Data Sold, Third-Party Marketing, Traditional Advertising, Behavioral Advertising, Data Profiles, Third-Party Tracking, and Track Users.

The rating question findings illustrate a wide range of changes:

1. *Since 2020 the **Sell Data** question indicates "worse" practices have increased to 14%.*

A continued increase in transparency has resulted in an increase in disclosures of "worse" practices. Since 2020 we see an approximate increase of 56%, from 9% to 14%, of products that disclose they sell data. Since 2018, we have seen an approximate 11% increase in products that disclose they do not rent, lease, trade, or sell data, representing the majority of products (72%). Unfortunately with the increasing transparency since 2018 we observe an approximate increase of 600% of products and services indicating they sell data (14%). Despite the increase in transparency, 14% of products and services remain "unclear" on data selling practices.

2. *Since 2020 the **Third-Party Marketing** question indicates "worse" practices have increased to 43%.*

A continued increase in transparency has resulted in an increase in disclosures of "worse" practices. Since 2020 we have seen an approximate increase of 7% of products that disclose they do not allow third-party marketing, representing 40% of products. Unfortunately with the increasing transparency since 2018 we observe an approximate increase of 13% of products indicating they allow third-party marketing (43%). Despite the increase in transparency, 17% of products and services remain "unclear" on third-party marketing practices.

3. *Since 2020 the **Traditional Advertising** question indicates "worse" practices have increased to 55%.*

A continued increase in transparency has resulted in an increase in disclosures of "worse" practices. Since 2020 we have seen an approximate increase of 4% of products that disclose they do not allow contextual or traditional advertising, representing 24% of products. Unfortunately with the increasing transparency since 2018 we observe an approximate increase of 38% of products indicating they allow contextual or traditional advertising (55%). Despite the increase in transparency, 21% remain "unclear" on contextual or traditional advertising practices.

4. *Since 2020 the **Behavioral Advertising** question indicates "worse" practices have increased to 47%.*

A continued increase in transparency has resulted in an increase in disclosures of "worse" practices. Since 2020 we have seen no increase in products that disclose they do not display targeted or behavioral advertising, representing 41% of products. Unfortunately with the increasing transparency since 2018 we observe an approximate increase of 62% of products indicating they display targeted or behavioral advertising (47%). Despite the increase in transparency, 12% remain "unclear" on whether they display targeted or behavioral advertising.

5. *Since 2020 the **Data Profile** question indicates "worse" practices have increased to 39%.*

A continued increase in transparency has resulted in an increase in disclosures of "worse" practices. Since 2020 we have seen an approximate decrease of 12% of products that disclose they do not create advertising profiles, representing 36% of products. Unfortunately with the increasing transparency since 2018 we observe an approximate increase of 290% of products indicating they do create advertising profiles (39%). Despite the increase in transparency, 25% remain "unclear" if they create advertising profiles.

6. *Since 2020 the **Third-Party Tracking** question indicates "worse" practices have increased to 55%.*

A continued increase in transparency has resulted in an increase in disclosures of "worse" practices. Since 2020 we have seen an approximate decrease of 6% of products that disclose they do not engage in third-party tracking, representing 31% of products. Unfortunately with the increasing transparency since 2018, we observe an approximate increase of 49% of products indicating they engage in third-party tracking (55%). Despite the increase in transparency, 13% remain "unclear" on third-party tracking practices.

7. *Since 2020 the **Track Users** question indicates "worse" practices have increased to 48%.*

A continued increase in transparency has resulted in an increase in disclosures of "worse" practices. Since 2020 we have seen an approximate decrease of 6% of products that disclose they do not track users on other applications and services across the internet, representing 34% of products. Unfortunately with the increasing transparency since 2018 we observe an approximate increase of 130% of products indicating they do track users on other applications and services across the internet. Despite the increase in transparency, 18% remain "unclear" on tracking practices.

Kids' Privacy Trends

Our findings indicate that the State of Kids' Privacy has been more transparent since 2018, with overall evaluation median scores increasing by approximately 20% from 41% to 49%. However, since 2020, overall median scores remain stable at 49%. Our findings also indicate that with increased transparency comes an increase in companies disclosing "worse" practices for kids and families, especially for the most critical practices regarding privacy. It appears companies are slowly integrating more forms of data monetization into their products year-over-year, or are being more transparent about their existing practices such as more selling of data to third parties, more targeted advertising using personal information, and sending more third-party marketing communications. Companies also appear to be integrating more indirect advertising and monetization business models, or are being more transparent about their existing practices such as the use of third-party tracking technologies that follow users on other applications and services across the internet for advertising and profiling purposes.

The State of Kids' Privacy indicates a widespread lack of transparency and a failure to protect children and students with better practices that apply to all users of a product.

Since 2018, companies have increased transparency in their policies to say they engage in third-party tracking of users; this also allows third parties to track users for their own advertising purposes. This could be the result of the market for data tracking and advertising network analytics maturing, with more options for companies looking to outsource this form of data monetization using more sophisticated offerings such as data profiling and long-game marketing. In addition, some companies may be making a shift to a data monetization practice that is less visible than displaying ads to its users, due to fewer regulations with respect to third-party data use and tracking as opposed to the greater number of regulations on first-party data use and advertising.[8] However, some companies are empowering users to push back. Apple's recent launch of its App Tracking Transparency (ATT) feature requires

[8] Ovide, S., *A Thumbs Down for Streaming Privacy*, The On Tech Newsletter, https://www.nytimes.com/2021/08/24/technology/streaming-privacy-data.html.

products to request that iOS users opt in to allow a product to track them for advertising purposes using the Identifier for Advertisers (IDFA), which is a unique device identifier Apple generates and assigns to every device. However, there are still other forms of third-party tracking technologies available to companies beyond the IDFA, and many are in use in products that are intended for children and students.

There has also been a notable shift by the industry to carve out exceptions in their products such as selling data or tracking teen or adult users for advertising purposes, but not selling data or tracking users of the product that are known to be under 13 years old. Companies have also increased their transparency indicating "worse" practices only apply to users who are not kids. For example, companies' policies have been updated to carve out exceptions that prohibit selling children's data, not displaying targeted ads to children, and not tracking child users of the product when the company has actual knowledge the user is a child or student. However, approximately half of all companies in 2021 likely avoid obtaining actual knowledge of whether a user is a child under 13 years of age through the product's experience with an age-gate or required birth date, which can lead to inadvertently exposing children using these products to data monetization practices that are intended to only apply to teen and adult users. Rather, companies likely have *constructive knowledge* that children under 13 are using their products — information that a company is presumed to have, regardless of whether or not they actually do. If a product has features such as child profiles, content directed to children, cartoons, or interactions clearly intended for children or that would likely appeal to children under 13 years of age, companies should know children are using the respective product and put in place stronger privacy protections.

METHODOLOGY

Our evaluation process for 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 a child's home address or other types of personal information. Therefore, our evaluation process pairs a transparency evaluation with a qualitative evaluation, which provides the ability to track the practices a policy discloses and the qualitative details of those policies, as discussed further in the Evaluation Process section below. The Common Sense evaluation process is completed with an attention to accuracy and fidelity that could withstand scrutiny including policy annotations associated with every question we answer. Full evaluations are completed by members of the privacy team who are licensed attorneys and are considered experts in privacy law, and every evaluation is reviewed by a second team member before being published.

Lastly, our evaluation process includes 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 identifying any potential 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.[9]

Among the applications and services we evaluated for this report, all of the products did 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. Products with no policy receive an automatic Fail rating. 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 achieve a *Fail* rating are underrepresented in our analysis. For comparison, as of the publication date of this report we currently have published over 1,000 privacy evaluations on our Common Sense Privacy Program website with less than 5% earning a *Fail* rating.

Additionally, our findings may not reflect all of the actual usage by applications and services given that additional and private student data privacy agreements may exist between the company and schools or districts. These additional agreements

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

not publicly available may add provisions as to how student information can be collected, used, and disclosed beyond the general provisions in the publicly available policies. Common Sense does work closely with schools and districts to get feedback on product use in the classroom as well as parental feedback on actual use by kids. In addition, many popular applications or services not included in this report are available to the public without sufficient policies available. In many instances, popular applications or services do not provide privacy policies prior to use, may provide broken links to policies, or do not contain policies at all.

Products We Rate

The Common Sense Privacy Program evaluates several different types of products. We evaluate popular education technology applications and services ("EdTech") that are currently used by tens of millions of students in classrooms across the country. Education-related applications and services used in schools and districts include a wide range of educational technologies such as games and tools for communication, collaboration, formative assessment, student feedback, content creation, and delivery of instructional content. The Privacy Program also evaluates popular consumer technology applications and services that are currently used by millions of children at home and in the classroom ("Kids' Tech"). Kid-related applications and services used at home include a wide range of technologies such as games and apps for communication, collaboration with friends, content creation, and delivery of media entertainment.

The 200 products selected for this report are representative of various different categories of apps and services used by children and students in every major age group at home, on the go, and in the classroom. Please see the Product Population Demographics for more details of the changing population of products used in this report year-over-year. We selected products for evaluation that have the biggest impact on as many kids, students, and families as possible. Criteria for selection of the 200 products used for this report include an intersection of multiple factors:

1. the most unique visitors to top-200 Common Sense Education apps;
2. the most unique visitors to top-200 Common Sense Consumer apps;
3. Apple and Google Play Store overall top-100 free category and top-100 kids and education categories;
4. Google Play Family Program recommended apps for kids and students;
5. trending press articles about popular apps and privacy;
6. apps that receive privacy awards;
7. new popular app product launches;
8. products with adoption rates of millions or tens of millions of users;
9. products used by kids and families for distance learning; and
10. requests from our community group of products in use in schools and districts.

This community group is called the Common Sense District Consortium, and was developed as a focus group in 2014 to help inform our work and provide feedback from a community of privacy-focused educators. There are currently over 400 members representing privacy experts from large and small school districts across the country. [10]

The wide range of categories of products used in this report include applications and services used by children at home and students in the classroom that represent a cross-section of the real-world digital environment of products used in different contexts: activity monitoring, app platforms, ebooks, classroom management, communication, computer programming, course feedback, educational analytics, educational content, educational curriculum, education games, educational intervention, educational resources, educational tools, financial education, kids' games, learning management systems (LMS), mental health,, music, news, parental controls, personalized learning, professional development, scholarship search, single sign-on, smart tech, social networks, streaming media apps, streaming learning content, student assessment, student engagement, utilities, virtual reality, and voice assistants.

To effectively evaluate the policies of all these different types of applications and services, we developed a comprehensive assessment framework based on existing federal and state law, as well as

[10] Common Sense Media, *Get Involved: For Districts and Schools*, Privacy Program, https://privacy.commonsense.org/resource/for-districts-and-schools.

on universal privacy and security principles. This framework incorporates more than 150 privacy- and security-related questions that are commonly expected to be disclosed in companies' policies in an educational or child-specific context. In the past year alone, parents and educators have been facing new challenges and privacy risks when it comes to balancing the power of online learning with the requirements of and concerns about online privacy.

Evaluation Process

The Common Sense Privacy Program created a comprehensive evaluation process for mobile applications and online services that attempts to address some of the common barriers to understanding a product's privacy practices. The privacy evaluation process includes questions organized into categories and sections derived from the Fair Information Practice Principles that underlie international privacy laws and regulations. Please see figure 227 in the Appendix for more details. In addition, the full evaluation 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. 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 company collects personally identifiable information (PII)?

If the reviewer responds yes to this question in our policy annotator software, that means the application or service discloses whether or not it collects personally identifiable information. Again given a 'yes' transparent response to this question the evaluator is then asked a follow-up question — a slightly adjusted version of the original attempting to capture if they engage in a particular practice. In this case:

Do the policies indicate the company collects personally identifiable information (PII)?

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. This includes questions where there is truly no qualitative value to a response and questions where determining if a given response is qualitatively "better" or "worse" requires additional context outside the scope of the evaluation process. The question process may seem slightly redundant having both a transparency and a qualitative component, but separating the disclosure from the actual practice engaged in provides an important metric for which portions of a policy may discuss a given practice. This distinction has proven valuable especially for products with overly complex or contradictory terms where identifying the actual practice presents a separate challenge.

Evaluation Framework

The privacy evaluation process utilizes our policy annotator software, which allows evaluators to read a company's privacy policy and annotate sections of relevant text for each of our evaluation questions, working toward an overall score and rating. The 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 company'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 clearly address the issue(s) raised in the question? The evaluator is looking to determine whether the policy addresses the issue, but also whether the issue is addressed clearly and without contradiction in another section of the policy or another policy.
    b. Qualitative selection: Do the policies indicate whether or not the company engages in the practice described?
    c. Notes: Is there anything noteworthy, exceptional, or egregious regarding the details of the question that should be recorded?

d. Policy references: Can the evaluator identify and select text within the policies to highlight and associate with the particular question?

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

In addition to engaging in this evaluation process, our team also published a basic Information Security Primer.[11] 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 inform more detailed observational testing.[12]

Basic and Full Evaluations

There are two types of privacy evaluations: basic evaluations and full evaluations. Both types of evaluations have the same rating icons and use the same overall scoring process. Basic evaluations are a 34-point inspection of the most important privacy and security questions about a product. Full evaluations are a 155-point inspection of all the comprehensive privacy and security full evaluation questions about a product, including all questions covered in a basic evaluation. Basic evaluations answer the most critical privacy and security questions about a product to determine an overall score, concern scores, and which rating they achieve in order to allow parents, teachers, schools, and districts to make an informed decision about whether to use the product. However, basic evaluations do not answer all the questions of a full 155-point inspection evaluation of a product, but still display an overall score and concern scores based on answers to only the basic evaluation questions. Basic evaluations can still be easily compared to basic or full evaluations because they share the same Evaluation Scores, Evaluation Concerns, Evaluation Ratings, and a subset of the Standard Privacy Report.

Basic evaluations were developed in response to multiple stakeholder queries for faster turnaround on evaluations, but we still use full evaluations for research purposes as they provide more detail for analysis on all the issues disclosed in a company's policies. Each basic evaluation question was carefully selected to balance the issues raised in the questions across all of the 10 different concern categories and filtered through the full evaluation Fair Information Practice Principles to create a representative sample of a full evaluation with only a limited number of questions.

Evaluation Scores

Every product with a privacy rating includes an overall evaluation score. A higher score (up to 100%) means the product provides more transparent and comprehensive privacy policies with "better" practices to protect user data. The overall score is not an average of the Evaluation Concern scores, but rather is a percentage of the number of points earned for basic evaluation questions. The score is best used as an indicator of how much additional work a person will need to do to make an informed decision about a product. This use is directly related to the core work driving the evaluations: to help people make informed decisions about a service with less effort. The higher the number, the less effort required to make an informed and appropriate decision. Every published privacy evaluation on our website displays the product's basic evaluation score derived from a 34-point inspection of the most important privacy and security basic evaluation questions about a product. The basic evaluation is a subset of a full evaluation. Therefore, products that received either a basic evaluation or full evaluation display the same basic evaluation score on our website to more easily allow parents, educators, and consumers to compare products using the same score based on the evaluation questions that matter most to them when making an informed decision to use the product themselves or with their children or students. However, the basic score is not a substitute for a full 155-point inspection of all the comprehensive privacy and security full evaluation questions about a product, which is why only products that receive a full evaluation are used in this report. For each question, the score is calculated as shown in table 1.

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

[12] *See* Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). Privacy of Streaming Apps and Devices: Watching TV that Watches Us. San Francisco, CA: Common Sense Media, https://www.commonsensemedia.org/research/privacy-of-streaming-apps-and-devices-2021.

Table 1: Explanation of scoring methodology

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

Each question contributes one point to the overall possible score and a score is calculated by totalling 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 evaluation concern scores utilize 10 questions and our evaluation statute scores are calculated against the respective number of questions in each privacy law. For the overall evaluation process, "Transparency" is defined as a measure indicating, of the things we expect to know, whether they are discussed in a company's privacy policies. In addition, "Quality" is defined as a measure indicating, of those things we know about, whether the company's disclosure about those practices protects personal information, which is considered qualitatively "better."

Our privacy-evaluation process for an application or service is unique because it produces a score based on both transparency and quality, which are combined into an overall score. These two metrics allow for an objective comparison between applications and services based on how transparent their policies are in explaining their practices and on the quality of those practices. Other privacy policy assessment tools have used algorithmic qualitative keyword-based contextual methods that attempt to summarize a policy's main issues. These keyword-based methods, such as Terms of Service; Didn't Read[13], and the Usable Privacy Policy Project[14], have been found to produce reliable measures of transparency information about the key issues disclosed in an application or service's policies. However, these methods are not able to capture substantive indicators that describe the meaning or quality of those disclosures. Therefore, our privacy-evaluation process was developed with this limitation in mind to incorporate both qualitative and quantitative assessment methods to appropriately capture the meaning of each privacy practice disclosed in a company's policies.

[13] Terms of Service; Didn't Read, https://tosdr.org.

[14] The Usable Privacy Policy Project, https://www.usableprivacy.org.

Overall Scores

To explain how evaluation questions affect an overall score, we present question 3.2.4 Third-Party Marketing from our published list of questions:

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

At a high level, this question has three possible responses:

1. The policies clearly indicate that personal information is shared with third parties for advertising or marketing purposes.
2. The policies clearly indicate that personal information is not shared with third parties for advertising or marketing purposes.
3. The policies do not clearly indicate whether or not personal information is shared with third parties for advertising or marketing purposes. Or, the policies have contradictory or "unclear" information regarding personal information sharing with third parties for advertising or marketing purposes.

The first option – if a company clearly indicates that they do share personal information for marketing purposes – still earns points toward the overall score even though it is a privacy-compromising practice, because the disclosure helps a person make an informed decision. Because we look at privacy through the lens of making an informed decision, we prioritize transparency in policy disclosures as a necessary requirement to make informed decisions. We acknowledge that this presumes a well-educated, informed consumer with market power, and that not all consumers have these resources. Still, we hope that this crucial piece of information is transformative in the market; it at least lets consumers know what transactions involving their personal information are happening. The second option – clearly specifying that personal information is not shared for marketing purposes – increases the

overall score the most, since that is a "better" practice that protects personal information the most. The third option – not sharing any information – brings the overall score down the most, because without any, or contradictory, information, making an informed decision is not possible.

Concern Scores

The privacy evaluation process summarizes the policies of an application or service into concern categories based on a subset of evaluation questions that can be used to quickly identify particular strengths and weaknesses of a company's policies. These concerns are composed of evaluation questions that can be used to calculate scores relative to that concern. As mentioned above, a basic evaluation does not have all questions answered, but each concern has at least some basic evaluation questions included to provide some indication of the policies relative to the given concern. A concern with all the full evaluation questions answered provides a more comprehensive analysis and understanding of an application or service's policies with respect to the specific concern. In addition, the 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.

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. The ratings and scores for each evaluation concern category are described below with a range of "best" to "poor":

- Best (81-100)
- Good (61-80)
- Average (41-60)
- Fair (21-40)
- Poor (0-20)

Products that score a "poor" are not necessarily unsafe, but they have a higher number of privacy problems or unknown practices than the "average" product. Similarly, products that score "best" are not necessarily problem-free, but have relatively fewer problems or unknowns compared with other products.

Statute Scores

Several statutes related to children and education are associated with one or more evaluation questions. As such, we can calculate scores for each statute or regulation using the 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.

However, these statute scores only provide an indication of how much additional work may be required to determine if an application or service is in compliance with respective international, 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.

Standard Privacy Report (SPR)

Privacy policies are often long and difficult to read, but – just like nutrition labels – they are also a critical piece that informs parents and educators about which data each product collects and which promises a company makes about how they use that data. Just like nutrition labels, privacy policies are meant to be read before the product is used, not after. When companies create a privacy policy for a product, they need to consider hundreds of issues, such as the intended users, the types of data the product collects, third parties that data is shared with, and how the company or third parties can use the data.

We spoke with hundreds of parents and educators who told us that reading and understanding privacy policies is hard enough, but trying to compare the privacy practices of multiple products in a standard way is close to impossible. As a result, we designed our privacy ratings and a standard privacy report to simplify the process of understanding privacy practices and displaying a product's expected privacy practices in a single format – much like a nutrition label – to help parents, educators, and companies understand the unique privacy practices of a product and easily compare privacy practices between products.

The standard privacy report (SPR) displays all the privacy practices of a product's policies in a consistent easy-to-read outline that can be compared to other products. The SPR indicates whether or not a product's policies disclose that they engage in each particular privacy practice and displays an alert icon when users should further investigate particular details prior to use. The alert icon indicates that the particular practice is either risky or "unclear." If a particular practice says "Did not evaluate," that means questions related to the practice were not included in our basic evaluation questions. Note that "Did not evaluate" does not necessarily mean that a service's policy does not comply with that individual practice, but rather it did not influence the scoring or other evaluation metrics. Only basic evaluations will include the "Did not evaluate" phrase, and only for questions that are not part of a basic evaluation.[15]

The SPR displays all of the findings from our 156-question full 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 answers to all of the full evaluation questions, including all of the basic evaluation questions, for easier comparison between products.

The SPR consists of all the privacy evaluation questions with answers about the privacy and security practices of a product's privacy policies. Readers have several options for navigating these questions and learning more about data privacy. Each of the possible answers to SPR questions include: "does" engage in the practice, "does not" engage in the practice, is "transparent" or "non-transparent" about the practice, and "did not evaluate" because we did not evaluate that question.[16]

Evaluation Ratings

At home and in schools and districts, parents and educators make decisions about privacy based on their specific needs. The privacy evaluation process is designed to support families and educators in making informed choices about the media and technology they use with kids at home or in the classroom. Our expert evaluators read the privacy policies and terms of use for hundreds of products in order to evaluate those tools across key privacy concerns. Then, each tool is assigned one of the following ratings:

1. *Fail*, which indicates that the application or service does not have a detailed privacy policy;
2. *Warning*, which means the product does not meet our recommendations for privacy and security practices; and
3. *Pass*, which means the product meets our minimum requirements for privacy and security practices.

Fail

Does not have a privacy policy and should not be used.

Technologies receiving a *Fail* rating have issues regarding whether a detailed privacy policy is available for evaluation. "Unclear" or qualitatively poor responses to the question listed below trigger inclusion in the *Fail* rating:

1. Is a privacy policy available?

The Fail Criteria for the *Fail* rating measures whether or not a company has done the bare minimum to provide users with a rudimentary understanding of how the company protects user privacy. Applications and services that do not meet this basic requirement can run afoul of federal and state privacy laws. As of 2021, among the applications or services we evaluated, less than 5% 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 *Warning* criteria described below, a *Fail* designation is not a sign that a company is necessarily doing anything illegal or unethical, but it could

[15] *See* Common Sense Media, *Privacy Evaluation for Example of Better Practices with Pass Rating*, Privacy Program, https://privacy.commonsense.org/privacy-report/Example-of-Better-Practices-with-Pass-Rating.

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

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 their services do not provide adequate expectations of how personal information will be collected or used.

Warning

Does not meet our recommendations for privacy and security practices.

Applications and services with a *Warning* rating have potentially risky or "unclear" practices in our Warning Criteria regarding data use, such as 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 company that builds the service) and third parties (any company given access to data by the company). Using data to profile children or students for advertising purposes can potentially violate multiple state laws and in some cases federal law. An application or service can be designated *Warning* for either a lack of transparency around data use – which creates the potential for profiling and behavioral targeting – or for clearly stating that 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 any of the questions listed below trigger inclusion in the *Warning* rating:

1. Effective Date: Do the policies clearly indicate the version or effective date of the policies?
2. Sell Data: Do the policies clearly indicate whether or not a user's personal information is sold or rented to third parties?
3. Third-party Marketing: Do the policies clearly indicate whether or not a user's personal information is shared with third parties for advertising or marketing purposes?
4. Behavioral Ads: Do the policies clearly indicate whether or not behavioral or contextual advertising based on a user's personal information is displayed?
5. Third-party Tracking: Do the policies clearly indicate whether or not third-party advertising services or tracking technologies collect any information from a user of the application or service?
6. Track Users: 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. Data Profile: Do the policies clearly indicate whether or not the company 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 *Warning* is not necessarily a sign that a company 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").

Pass

*Meets our **minimum** requirements for privacy and security practices.*

Applications and services with a *Pass* rating have met a minimum criteria for transparency and "better" practices in their policies in our Pass Details. Before using an application or service with this rating, 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, potential users of a product are encouraged to review context-specific issues or concerns before any child or student data is shared with a service.

Responses to the questions listed below are displayed on the Common Sense Education edtech reviews to provide more detail about a product with a *Pass* rating that are of relevance in an educational setting:[17]

1. Children Intended: Do the policies clearly indicate whether or not the product is intended to be used by children under the age of 13?
2. Collection Limitation: Do the policies clearly indicate whether or not the company limits the

[17] Common Sense Education, *Edtech Reviews*, https://www.commonsense.org/education/search?contentType=reviews.

collection or use of information to only data that is specifically required for the product?

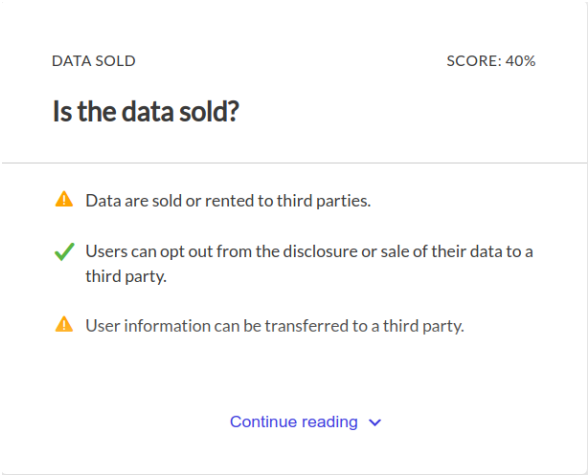
3. Safe Interactions: Do the policies clearly indicate whether or not a user can interact with trusted users?
4. Visible Data: Do the policies clearly indicate whether or not a user's personal information can be displayed publicly in any way?
5. Breach Notice: Do the policies clearly indicate whether or not the company provides notice in the event of a data breach to affected individuals?
6. Parental Consent: Do the policies clearly indicate whether or not the company or third party obtains verifiable parental consent before they collect or disclose personal information?

Rating Risks

A comprehensive privacy risk assessment can identify risks and determine areas of concern in order to minimize potential harm to children and students. Children require specific protection of their personal information, because they may be less aware of the risks, consequences, safeguards, and concerns as well as their rights in regards to the processing of their personal information. The Common Sense 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 rating icons described below, 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 rating icons, our privacy evaluations display rating 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 company's practices may be cause for 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 ratings and allows those who are curious about why we gave a product a particular rating to see which factors deserved special notice and are therefore marked with a yellow alert icon.

Figure 3: Example of yellow alert icon indicating "worse" or "unclear" practice, and green check mark indicating "better" practice.



The following rating 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.

Fail Criteria

Figure 4: Fail rating image

The following single criterion is used in the determination of whether or not a product receives a *Fail* rating for lack of a privacy policy 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 may cause harm.

Warning Criteria

Figure 5: Warning rating image

The following seven criteria are used to determine whether a product receives a *Warning* rating for "unclear" or "worse" practices.

- **Effective Date**: A child or student's personal information should not be collected or used by a product that does not indicate the date or version of the policies, because there is no notice of when the policies were changed and no expectation of trust that a product can change how they use data. The effective date is important to disclose because it provides notice to users if, and when, the terms of a product changed. If a policy's effective date changes, that could also mean that the data collection practices of the product may also have changed and could impact a user's privacy.
- **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 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 in order to influence their ideology or desire to purchase goods and services.
- **Third-Party Tracking**: The company 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.

Pass Details

Figure 6: Pass rating image

If a product does not flag any of our criteria for the Fail or Warning ratings, it has met our minimum safeguards and is rated *Pass*. The *Pass* rating does not have explicit criteria of its own because privacy concerns and needs vary widely based on the type of application or service and whether the app is used at home or in the classroom. As a result, we have highlighted the following best practices for additional consideration on the Common Sense Education edtech reviews that are of relevance in an educational setting: use by children, limiting the

collection of personal information, not making information publicly visible, safe interactions, data breach notification, and parental consent.

- **Children Intended**: A company 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.

Concern Categories

Parents and educators share common concerns about the privacy and security practices of technology used by their children and students. Based on these concerns the Privacy Program created the following 10 privacy evaluation concern categories. Each privacy concern category is intended to allow for a more narrow evaluation of the strengths and weaknesses of a product and how that application or service compares to similar products. Each privacy evaluation concern category is composed of 10 evaluation questions that provide a brief analysis of the most important privacy practices of a product. Depending on the type of privacy evaluation, either all of the 10 evaluation questions are used with a full evaluation, or only the most critical basic evaluation questions are used to make up a concern's score with a basic evaluation.

1. Data Collection: What data does it collect? Responsible data collection practices limit the type and amount of personal information collected about people to only what's necessary to provide the application or service.
2. Data Sharing: What data does it share? Data sharing best practices protect a person's personal information from being shared with third-party companies and advertisers.
3. Data Security: How does it secure data? Data security best practices protect the integrity and confidentiality of a person's data.
4. Data Rights: What rights do I have to the data? A person's data rights include the ability to review, access, modify, delete, and export their personal information and content.
5. Individual Control: Can I control the use of my data? A person has a right to exercise control over what personal data companies collect from them and how their information is used.
6. Data Sold: Is the data sold? Best practices include not sharing, renting, or selling a person's

personal information to third parties for financial gain.

7. Data Safety: How safe is this product? Data safety best practices limit the visibility of a person's information and their interactions with others to protect their physical and emotional well-being.
8. Ads & Tracking: Are there advertisements or tracking? Responsible advertising practices limit the use of personal information for any third-party marketing, targeted advertising, tracking, or profile generation purposes.
9. Parental Consent: Can a parent or guardian provide consent for their child? For use by children age 13 or under, a parent or guardian's verifiable consent is required before the collection, use, or disclosure of the child's personal information to an application or service.
10. School Purpose: Is the product intended for school? Data collection from K-12 students or teachers must abide by the legal obligations for the privacy and security of that educational information.

Privacy Audience

Privacy evaluations are designed to reduce the complexity of a product's privacy policies into a simple and consistent framework that provides the right amount of detail and information about a product for every user at the right decision point given their awareness and understanding of privacy. Our privacy evaluations aim to provide enough detail about a product to help potential users 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 is available. The privacy evaluations provide evaluation results based on a parent or educator's privacy awareness at the following levels: none, 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 may have never or have rarely taken the time to 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 the 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, are comfortable reading privacy policies, and look for as much detail as possible about a product to meet their federal, state, or contractual procurement requirements.

Table 2 describes how our privacy evaluation results break down into different levels of evaluation details based on an individual's privacy awareness:

Table 2: User awareness of privacy issues.

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

The vast majority of users are in the "No" and "Low" awareness categories with decreasing representation in each category as privacy complexity and compliance details increase. The privacy ratings describe how we categorize evaluations into three ratings: Fail, Warning, or Pass based on meeting minimum privacy and security requirements, which parents and educators, with no privacy awareness, can use to make a more informed decision. We also describe the difference between basic and full evaluations, and our Evaluation Scores section describes how overall scores can help parents and educators with low privacy awareness compare products and make an informed decision about a product's privacy practices alongside its evaluation rating. The

Rating Risks section also describes how our rating criteria help parents and educators with low privacy awareness quickly understand why a product received its rating with some helpful information to learn more about the privacy risks and harms.

Our evaluations also 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, as discussed in the Evaluation 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 Evaluation 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 who the policies specify are the intended users of an application or service, such as children, students, teens, parents, educators, or consumers.

For app developers, consumers, parents, and educators with high privacy awareness, the Evaluation Scores section describes how each concern category receives its own score based on how the company's policies answered the 10 questions in each concern, or fewer for basic evaluations. Similarly to rating 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 tells parents and educators with high privacy awareness that they can download a simple report that summarizes a product's policies in an easy-to-read bullet outline describing the privacy statements of the product. Moreover, for parents, educators, and school or district administrators with compliance awareness of privacy, our standard privacy report and privacy direct data export[18] 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, companies with compliance awareness can navigate the full evaluation questions, which include additional background information and relevant citations to help them learn about "better" practices for each evaluation question. Lastly, our Policy Annotator tool is available for parents, educators, and companies who would like to complete their own privacy evaluation and better understand the privacy practices of products they use every day.[19]

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. For example, 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. 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.[20]

[18] Common Sense Education, *Privacy Direct*, Privacy Program, https://www.commonsense.org/education/privacy-direct.

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

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

Mixed-Audience

A mixed-audience product is directed at children but does not target children as its "primary audience" – rather, it 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.

Selective Privacy

The Privacy Program only evaluates products that are considered general audience and mixed audience, which includes products directed at children and students, or would appeal to them. A child-directed product typically has a separate privacy policy and website, and the application or service has the same privacy protections for both children and students. However, general audience and mixed-audience products with various users often have different privacy practices and protections based on the category of user. This varying type of privacy practice allows the company to establish privacy protections that apply only to a specific subset of users. For example, some products may sell user data and display behavioral advertising to parents, teachers, and consumers but do not do so for children or students.

The Privacy Program evaluates products based on multiple dimensions that include an overall score, rating, and evaluation concerns, as described in our Evaluation Process 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 rating 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 general audience or mixed-audience product is intended for both children and adults but has different privacy practices for adults than for kids, our rating reflects any "worse" practices 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 child turns 13 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 ratings are designed to protect all users and flag a privacy risk if the risk applies to any intended user of the product. The following table 3 illustrates three examples of the different ratings a general audience or mixed-audience product could receive:

We believe this approach appropriately 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 users is afforded protections, we display potential issues if any users are at risk. This allows parents and educators to be appropriately informed about a product's overall privacy risks up front and provides 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.

Our approach also takes into account the possibility of extrapolation of a child or student's personal information in protected accounts by proxy or association with Managed Accounts that may not have the same privacy protections. For example, if a product has mixed privacy practices that include the use of

Table 3: Explanation of how ratings consider all users of a product for risk factors

Rating Flags	Rating	Details
None	Pass	If none of the rating criteria has been flagged with an alert icon, that means the answers to all the rating questions have been disclosed in a product's policy with "better" responses. This product would receive a *Pass* rating.
Apply to all users	Warning	If one or more of the rating criteria has been flagged a privacy risk, that product would be rated *Warning* – 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.
Apply to only a specific type of user	Warning	If one or more of the rating criteria has been flagged a privacy risk, that product would be rated *Warning*. However, if the privacy risks only apply to a specific type of user such as a parent or educator but do not apply to children and students, the product would still be rated *Warning*. This approach alerts all potential users of the privacy risks and also indicates in the product's overall summary any additional protections provided for other intended users.

"worse" practices for adult users such as behavioral ads or tracking, but does not use "worse" practices for child profile accounts, the product may still be able to indirectly track or target children or students on the product through a parent or educator's account.

Interpreting "worse" or Illegal Practices

The privacy practices of companies we evaluate are disclosed in their publicly available privacy policy, and they weave a complex and unique narrative that informs potential users about the company's story and its legal compliance obligations with federal and state privacy laws. The policies are intended to educate users about what data a company's product collects, how it uses that data, and whether it shares that data with third parties and for what purposes. A company's privacy policy and terms of use are also meant to create a legal contractual relationship between the company and each user based on the company's disclosed privacy practices and promises. Better privacy-protecting promises disclosed in a privacy policy are meant to persuade a wide range of users – consumers, parents, educators, and their children and students – to use a company's product and allow them to make an informed decision. However, "worse" privacy-regressive practices disclosed in a privacy policy are meant to inform users of the potential risks if they choose to use the product. When practices are not disclosed in a company's privacy policy there can be no expectation of how a user's data may be used by the company which we indicate as "unclear." A "worse" or "unclear" practice may not be a violation of the law. For example, if some users, like children or students, have Selective Privacy with "better" privacy practices under the law than other users such as consumers, parents, or educators, a product may maintain compliance by providing protections only for those users required by law while engaging in privacy-regressive practices for all other users. However, the presence of "worse" practices in a product is not an industry *best practice*, because it puts all users' privacy at risk, especially that of children and students if they are inadvertently exposed to "worse" privacy practices intended only for other users who are not protected under federal or state privacy laws.

Our privacy evaluation results are meant to only highlight "worse" practices of products used by kids and families and do not make any legal determinations on whether a company has actually violated the law.

Our evaluation results in this report are not meant to definitively state whether a company has engaged in illegal practices in violation of either state or federal law, or agency regulations. Rather, our privacy evaluations are meant to only highlight "worse" practices for kids and families in the privacy policies of companies which indicate there *may* be a potential violation of the law if those "worse" practices apply to

a particular type of user, in a particular context, and for a particular prohibited use.

Whether or not a company's "unclear" or "worse" practices in their policy actually indicate they have engaged in illegal practices in violation of federal or state law is a legal determination as a matter of law that can only be made in a legal proceeding by a court appointed judge or agency regulator. Furthermore, a determination on whether a company has violated the law requires a legal proceeding that examines the evidence of a company's promises in its privacy policy against observational direct evidence obtained through a legal investigation with subpoena power of the company's confidential product source code, servers, systems, employees, and third-party data sharing agreements to determine how users' data is collected and used.

Therefore, the following results only serve to direct policymakers, judicial representatives, and regulators to the privacy issues and concern categories across the industry to better direct their limited resources and understand the state of kids' privacy. Additionally, products with Selective Privacy practices create both implementation challenges and usability issues for ensuring students' and children's privacy is protected and products are being used in a privacy-protecting manner.

RESULTS

This report should not only be used as a means to inform individuals about the general state of privacy practices in the kids' tech and edtech 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 Privacy Audience, we are extremely cautious 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 safety or 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 especially when changes we see might be reflections of changes in our methodology – see Product Population Demographics in the appendix for further consideration. Evaluations that receive our full, rather than basic, evaluation do experience a selection bias in several ways:

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

As such, it should be expected that our analysis likely overestimates industry practices in a positive direction, especially for data prior to 2020 that was focused more on products for use in the classroom than kids' tech products used at home. It would also 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 are posed by increasing the number of products evaluated, as well as the scope of products evaluated. In 2018, the report included 100 evaluations of the most popular applications and services used by students in K-12 schools and districts. In 2019, we included an additional 55 products and removed the five products that were discontinued, for a total of 150 products evaluated. In 2020 we added 50 more products. In both 2020 and 2021 we evaluated 200 products each year, with several products discontinued each year and new products with increasingly high adoption by children and students taking their place. Given such a large increase in the number of products evaluated from 2018 to 2020 as well as the expanded scope of products evaluated in 2020, some of our findings may indicate an unintended selection bias on our part as well as general shifts in the industry. Where possible, we attempted to verify that any trends we discussed were also trends seen in our sub-population of products evaluated all four years. We have done our best to ensure that our selection process has remained thoughtful and intentional year over year, with a population of products more likely to be used or considered for use in

the classroom in 2018 and 2019, and the addition of more kids' tech products more likely to be used at home in 2020, to create a more representative sample of the current environment of the most popular applications and services used by children and students. All of the companies evaluated in 2021 are listed in the Appendix in the List of Products Evaluated 2021 section. However, some of our results will likely be an indication of unintended biases due to changes we made, which we will continue to analyze in our research and explicitly flag where general trends vary significantly from our trends seen in products evaluated all four years.

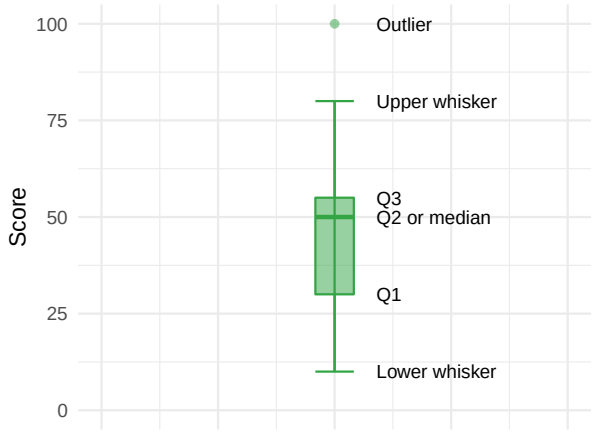
For example, products evaluated every year since 2018 have included more traditional edtech-classified companies that disclosed in their policies that they were intended for use in schools with students. In 2019, we added a mix of new products that would likely be classified as both kids' tech and edtech, with the intended audiences primarily focused on children or students. In 2020 and 2021, more products were added that would likely be classified as more kids' tech, with fewer disclosures relating to school or district use to create a more representative distribution and environment of kids' tech used by children at home and edtech used by students in the classroom. That said, we see several areas that remain consistent as well as several areas where industry norms appear to be shifting ,with the edtech classification continuing to be blurred between products used by students at home and in the classroom.

In general, box plots and bar charts are used throughout the report to compare 2018, 2019, 2020, and 2021 data. All other graphs will tend to analyze 2021 data only to ensure we are assessing trends only where it is appropriate. Analysis that only includes 2021 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.

We include box plots for comparing year-over-year 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).

- 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.
- 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.
- 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).
- 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.
- 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 7: Example box plot



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 an indication whether those changes require an update of that product's privacy evaluation to reflect any changes in 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 are made, typically the changes are additions to the policy text that improve transparency around privacy practices the company may

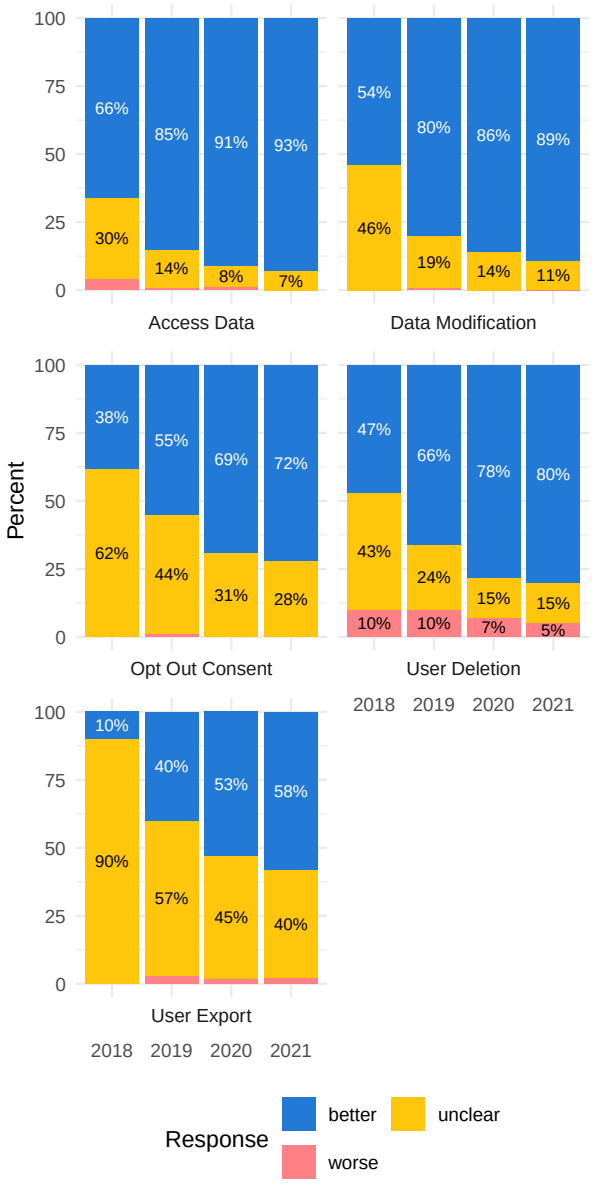
already engage in. Companies choose to make substantive changes to their privacy policies based on many factors, but typically we see changes made in response to customer questions about that company's specific practices, due to the addition of new features or products that change how the company collects or uses personal information, or for compliance purposes with changes in the law. Companies have been making substantive changes to their privacy policies at a rate higher than seen in previous years.

The Privacy Program found that over 50% of the 200 most popular applications and services evaluated in 2021 made substantive changes to their policies since 2020 with many companies changing the majority of their policy's text.

In some cases, companies update their policies several times each year. 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. 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.[21] In addition, California passed the California Consumer Privacy Act (CCPA), which provided many of the same privacy rights as the GDPR for California residents, as well as the right for consumers to provide opt-out consent from a company selling their personal information.[22] However, many companies created separate GDPR sections in their privacy policy or a separate CCPA policy that only applied the new privacy rights for users in those specific jurisdictions. For the purposes of our evaluation framework, we require a company to provide the same privacy rights to all users of the product to earn points, rather than only selectively to particular users in particular geographical jurisdictions.

Accordingly, our 2021 results as shown in figure 8 indicate an increase in transparency since 2018 and "better" disclosures for the following evaluation questions related to new privacy legislative requirements that required companies to update their policies to allow users to exercise their privacy rights: Access Data, Data Modification, User Deletion, User Export, and Opt-Out Consent in response to consumer awareness and complaints.

Figure 8: Transparency disclosure shifts related to legislative requirements year-over-year results



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

[22] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.198.

Policy Transparency

Transparency is a direct proxy for informed consent. The more transparency a company provides in its policies about its product's privacy practices, the more information parents, educators, and consumers have to make better choices for themselves, their children, and their students. Privacy policies are often long and difficult to read, but – just like nutrition labels – they are also a critical part of a product that informs users about what data the product collects and what promises a company makes about how they use that data.

As an analogy, when shopping for products in the store, some ingredients in a product are more important to some consumers than other ingredients are, such as whether the product contains wheat, dairy, nuts, or meat given that the shopper may have dietary restrictions or an allergic reaction to a particular ingredient. This analogy is useful in comparing the lack of transparency for an application or service relative to the different contexts in which it could be used, such as at home, in the classroom, at work, or in public places. In addition, products may be used by different audiences with different needs that may require different accommodations and protections, such as consumers, parents, educators, or their children and students.

All our evaluation questions – like ingredients – cover a wide range of unique issues that make up a comprehensive landscape of all the FIPPs privacy principles across privacy, safety, security, and compliance-related issues that would reasonably be expected to be disclosed in the privacy policies of products intended for children and students. Companies may incorrectly assume that users do not expect to see all the possible practices, or lack thereof, of a product in its privacy policy because they assume that like a nutrition label, listing all the ingredients a product does and *does not* contain would be too much information.

However, privacy policies and nutrition labels for products are not the same. If a product's nutrition label does not disclose that it contains a harmful ingredient consumers look for when making a decision on whether or not to purchase the product, such as wheat, dairy, or nuts, that means the product *does not* contain those potentially harmful ingredients and therefore the product does not pose a risk for that particular consumer.

Even more problematic is when companies cannot agree on a standardized definition of what an ingredient actually contains or even on the ingredient's origin, and may use multisyllabic and confusing names to describe ingredients. We see similar issues in the privacy landscape with obfuscating language, and in some cases a lack of vocabulary and societal awareness necessary to discuss issues in a consistent manner. This lack of consensus results in the use of different language to explain similar privacy practices, which further confuses consumers. A product's privacy policy that does not transparently disclose its "worse" practices that consumers look for when making a decision to use the product means the product should not be presumed safe, because the product still reserves the right to engage in the "worse" practice without any notice, putting children and students at risk for potential harm.

Regardless, for food labeling, some ingredients are so harmful to some people that top allergens are often explicitly disclosed for clarity (eg. Contains: Nuts, Dairy, Wheat, Soy). Many privacy issues pose similar risks and should be explicitly disclosed regardless of whether or not a practice is engaged in it.

Unlike a product's nutrition label, a company's privacy policy that is unclear or non-transparent regarding a privacy practice means the product may still engage in that practice without providing any additional notice.

The following analysis looks at the percentage of transparency across all our full evaluation questions (155), the basic questions (35), and our rating criteria questions (7) in order to determine if informed consent is possible across these different types of indicators.

All Questions

Figure 9 and table 4 indicate the transparency percentage aggregated across all the evaluation questions since 2018. The results indicate increasing transparency across all our evaluation questions. However, there is still a widespread lack of transparency, with only 63% median transparency per question in 2021. In addition, in 2021 the bottom 25% of our questions range from 4% to 38% transparency. The middle 50% of our questions range from 38% to 79% transparency, and the upper 25%

of our questions range from 79% to 100% transparency.

Companies need to do better to address their users' interests by being more transparent in their policies, rather than just disclosing details related to protecting their business interests.

Over half of our questions have a disclosure rate above 63%. This means that for many questions or practices, it is difficult to expect that you will have the information needed to make an informed decision. For comparison, when it comes to shopping for products in the store, different types of consumers would not realistically be expected to make an informed decision whether to purchase a product if approximately 30% of the nutrition label on the back of the product were blank or only listed 70% of the ingredients. Privacy policies are lacking even more information than this hypothetical shopping analogy.

Figure 9: Transparency analysis aggregated by question all questions

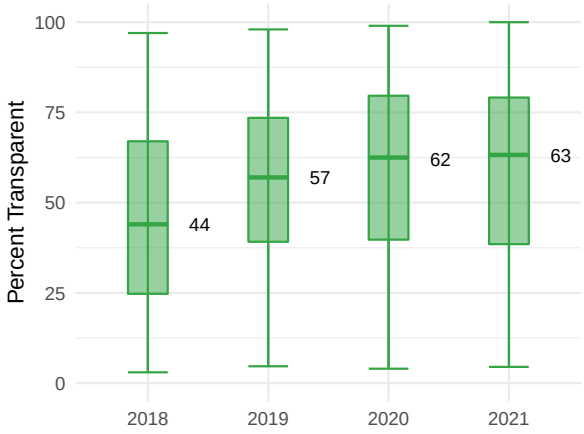


Table 4: Transparency analysis aggregated by question all questions descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	3	25	44	46	67	97
2019	5	39	57	55	74	98
2020	4	40	62	59	80	99
2021	4	38	63	59	79	100

Figure 10 and table 5 indicate the transparency percentage aggregated across all products since 2018. The results indicate that transparency in the industry relative to all our evaluation questions is increasing. However, there is still a widespread lack of transparency, with a median transparency per product of only 60% in 2021. In addition, in 2021 the bottom 25% of our products range from 17% to 51% transparency across all of our evaluation questions. The middle 50% of products evaluated range from 51% to 69% transparency, and the upper 25% of our products range from 69% to 100% transparency. However, transparency aggregated across products indicates extreme outliers on the low end, which means there are products that are far below the industry norm for transparency. Additionally, there is one extreme outlier product achieving 100% transparency across all of our evaluation criteria, indicating that it is not an impossible achievement and that all products should strive to be more transparent.

Figure 10: Transparency analysis aggregated by product all questions

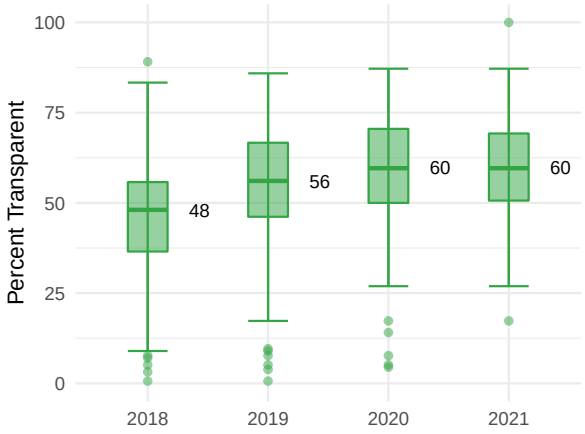
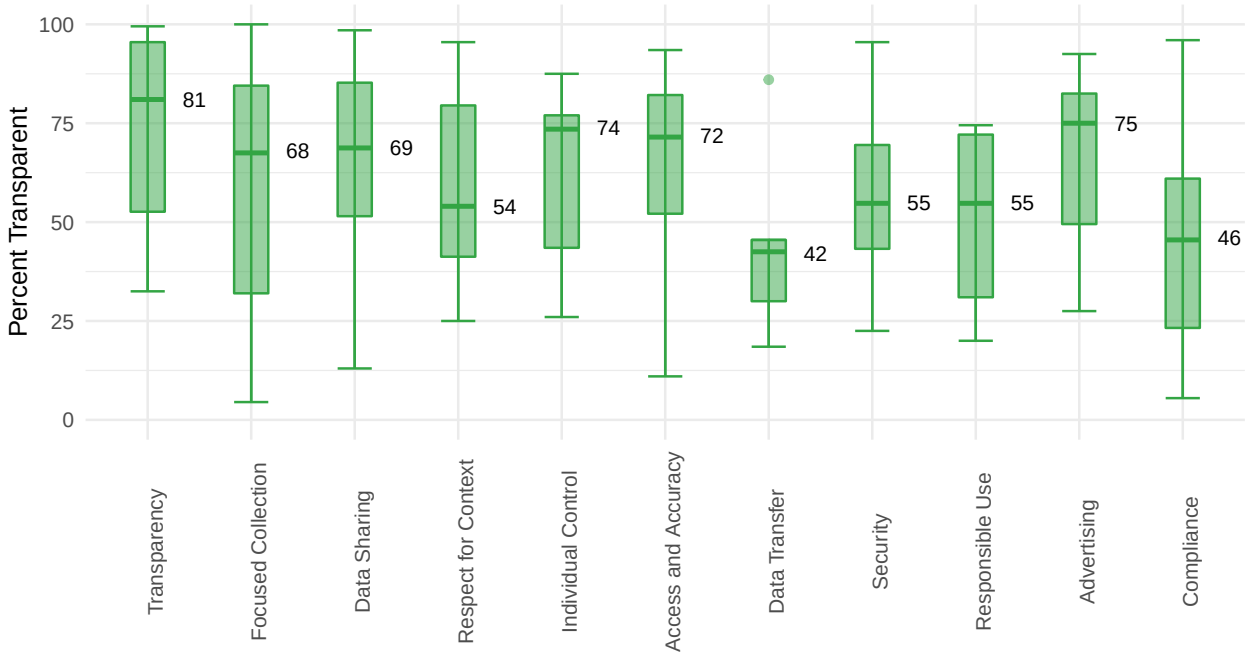


Table 5: Transparency analysis aggregated by product all questions descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	1	37	48	46	56	89
2019	1	46	56	55	67	86
2020	4	50	60	59	71	87
2021	17	51	60	59	69	100

We can also take a deeper look into how transparency is distributed across privacy principles in

Figure 11: Average percent transparency per question aggregated by respective FIPPs category



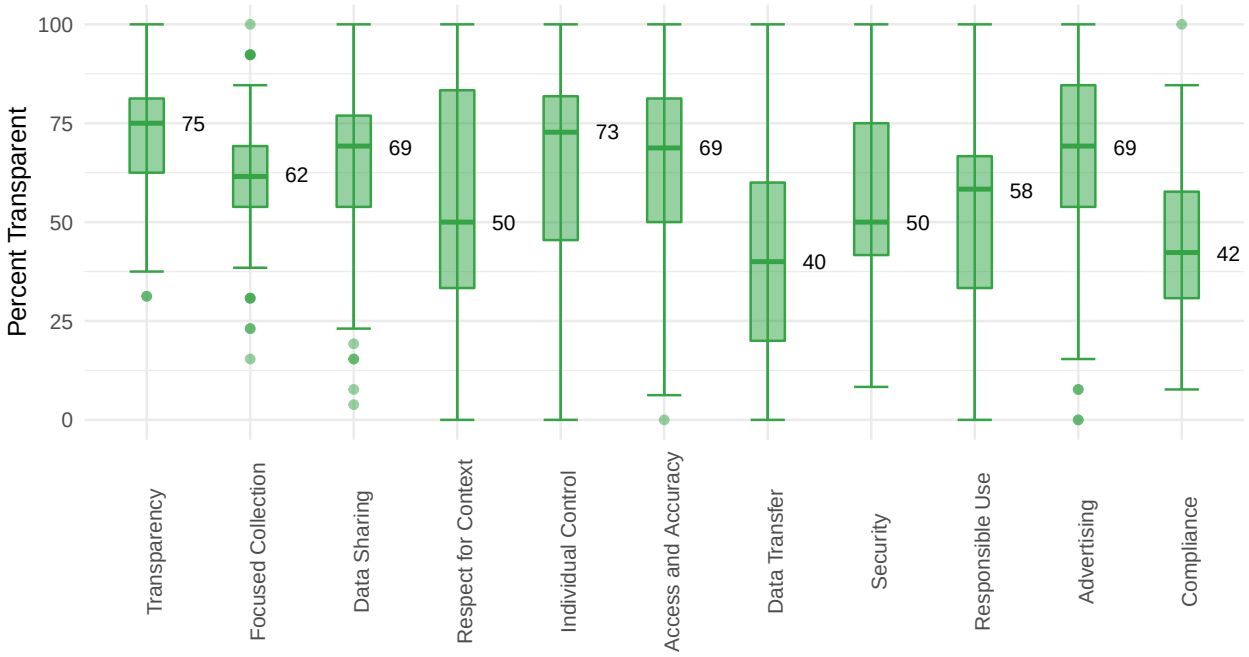
the next analysis, which breaks down the percent transparency aggregated by question, and then groups all the questions by their respective FIPPs category, to better understand the general trends relative to where transparency is particularly widespread or lacking. From the analysis as seen in figure 11 and table 6, we see 10 of the 11 categories with a median average question transparency below 75%, meaning that for a majority of the questions in the respective categories there simply is not enough information to inform decisions on whether or not a product is appropriate in a given context. Of particular note are the FIPPs categories Data Transfer and Compliance, which have an average question transparency median score below 50%. In the case of Data Transfer, this means there are not sufficient details about how a user's data will be transferred to third parties, and whether existing privacy protections are maintained after data is in control of a third-party in the case of a bankruptcy, merger, or acquisition. This is especially concerning given that 84% of products evaluated indicate they will Transfer Data to a successor third-party company in the event of a merger, acquisition, or bankruptcy.

Table 6: Average percent transparency per question aggregated by respective FIPPs category descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
Transparency	32	53	81	73	96	100
Focused Collection	4	32	68	60	84	100
Data Sharing	13	52	69	64	85	98
Respect for Context	25	41	54	59	80	96
Individual Control	26	44	74	63	77	88
Access and Accuracy	11	52	72	65	82	94
Data Transfer	18	30	42	44	46	86
Security	22	43	55	58	70	96
Responsible Use	20	31	55	50	72	74
Advertising	28	50	75	67	82	92
Compliance	6	23	46	44	61	96

In addition, the FIPPs Compliance category covers a broad range of issues that impact the privacy of children under 13 years of age and students in K-12 schools and districts. The category requires disclosure of how a product protects personal information from children and educational records of students, with additional focus on how parental consent is

Figure 12: Percent transparency per product grouped by FIPPs category



obtained and how student data privacy is protected. The category has a wide range of scores, but with a comparatively low median score of 46%. Companies are likely only disclosing the minimum compliance requirements they believe apply for either intended children or students using the product, but not both. This finding highlights the need for companies to increase their transparency on compliance-related details that apply to both children and students using their product, even if the company does not believe both children and students are intended users because the products evaluated in this report are the most popular products used by both children and students. Companies also need to go beyond disclosing only the minimum compliance requirements related to their product, and need to discuss more details on how privacy protections for children and students are actually implemented in the product.

In order to understand what the transparency landscape looks like at the individual product level, we also completed an additional analysis, as seen in figure 12 and table 7, by taking a deeper look at each product's respective FIPPs category transparency percentage and then providing descriptive statistics across all products. In many ways this analysis provides a similar picture as compared to the previous analysis. However, we can see that for some products there is a high level of transparency, indicating that our expectations for more transparency are not unreasonable. We see additional low transparency results in the Data Transfer and Compliance FIPPs categories as mentioned previously. In considering areas where products are trending toward more transparency, we see the Transparency and Focused Collection categories with a median product transparencies of 75% and 62% respectively.

Table 7: Percent transparency per product grouped by FIPPs category descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
Transparency	31	62	75	73	81	100
Focused Collection	15	54	62	60	69	100
Data Sharing	4	54	69	64	77	100
Respect for Context	0	33	50	59	83	100
Individual Control	0	45	73	63	82	100
Access and Accuracy	0	50	69	65	81	100
Data Transfer	0	20	40	44	60	100
Security	8	42	50	58	75	100
Responsible Use	0	33	58	50	67	100
Advertising	0	54	69	67	85	100
Compliance	8	31	42	44	58	100

For some products there is a high level of transparency across all details and concerns, indicating that our expectations for more transparency are not unreasonable.

For these FIPPs categories, products in general are providing a higher level of transparency across all products, and we see the collective group of products trending toward more transparency. These areas are fairly well understood and regulated and relatively easy to comply with through privacy policy disclosures, so products should have even a higher level of transparency. Most of the other categories indicate that there are no industry trends for transparency, as we see products spanning the whole spectrum from near 0% to 100% transparency.

Some areas show promise of increasing transparency or general industrywide trends such as the Advertising and Data Sharing FIPPs categories, because they appear to have some tendency toward general transparency with median average product transparency of 69% for both categories. However, this is likely due to recent privacy-focused legislation such as the CCPA and the subsequent CPRA that put pressure on companies to transparently disclose how data is shared with third parties for advertising purposes. More transparency in these FIPPs categories could help protect a company's advertising-related revenue streams, because they could argue that increased transparency provides adequate notice to users with informed consent for these "worse" practices regarding areas with increased consumer awareness and concern. The general lack of transparency in most privacy categories indicates more vendors need to spend additional time discussing issues relevant to the privacy of their users rather than minimizing their legal liability and protecting their revenue streams.

Basic Questions

Figure 13 and table 8 indicate the transparency percentage aggregated across all the basic questions since 2018. The results indicate increasing transparency across all the basic evaluation questions. However, there is still a widespread lack of transparency, with a median transparency of only 80% in 2021. In addition, in 2021 the bottom 25% of our basic evaluation questions range from 34% to 64% transparency. The middle 50% of our questions range from 64% to 89% transparency, and the upper 25% of our questions range from 89% to 100% transparency. Compared to the median transparency aggregated across all the evaluation questions of 62%, the smaller number of basic questions with median transparency at 80%, 12% points higher, indicates that the specific issues raised in our basic evaluation questions are more frequently disclosed in policies across the industry. The basic evaluation questions cover a much narrower range of issues, containing only 35 questions. Given that these questions are of such high importance to consumers, parents, and educators when making a decision whether to use a product, companies are expected to address every single issue in our basic evaluation process in their policies. Lastly, when there is such a high percentage of non-transparency across the basic evaluation questions, there is no reasonable expectation of how the product will collect and use personal information for any user.

Figure 13: Transparency analysis aggregated by question Basic questions

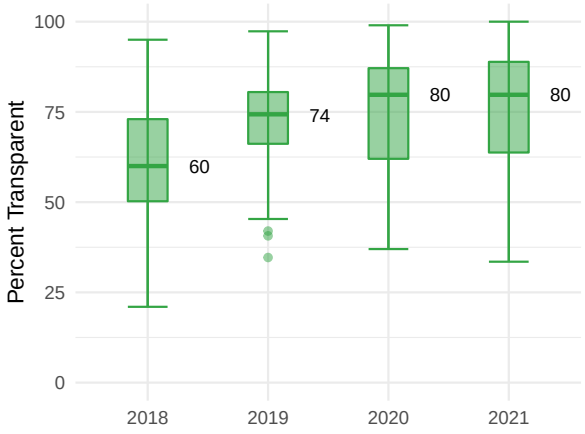


Table 8: Transparency analysis aggregated by question Basic questions descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	21	50	60	61	73	95
2019	35	66	74	72	80	97
2020	37	62	80	75	87	99
2021	34	64	80	75	89	100

Figure 14 and table 9 indicate the transparency percentage aggregated across all products since 2018 for our basic evaluation questions. The results indicate transparency in the industry relative to all our

basic questions is increasing. However, there is still a widespread lack of transparency, with a median transparency of only 76% in 2021. In addition, in 2021 the bottom 25% of products evaluated range from 12% to 65% transparency. The middle 50% of our products range from 65% to 88% transparency, and the upper 25% of our products range from 88% to 100% transparency. Our analysis also indicates extreme outliers on the low end, as indicated by dots in figure 14, which means there are numerous products that are far below the industry standard range of transparency on our basic evaluation questions. These companies need to do better to inform users about their various practices related to our basic evaluation questions.

Figure 14: Transparency analysis aggregated by product Basic questions

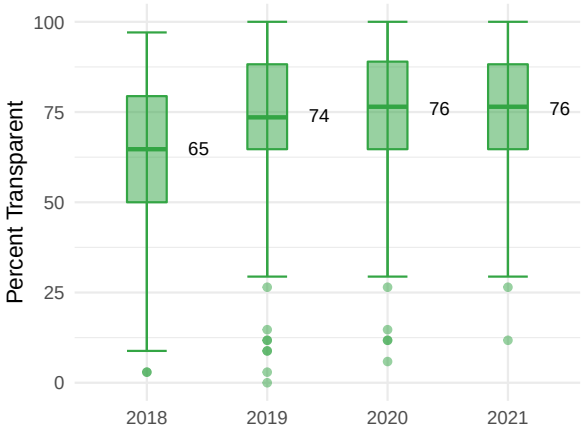


Table 9: Transparency analysis aggregated by product Basic questions descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	3	50	65	61	79	97
2019	0	65	74	72	88	100
2020	6	65	76	75	89	100
2021	12	65	76	75	88	100

Rating Criteria

All the full and basic evaluation questions cover a wide range of issues, but the rating criteria evaluation questions cover a very narrow range of the most critical issues across only seven questions. Companies are expected to address every single issue in our rating criteria in their policies, given the small number of questions and that these issues have the highest awareness and importance to consumers, parents, and educators when making a decision whether to use a product.

Not all products make clear promises about critical issues regarding safety and privacy for kids across all of our rating criteria.

Across all rating criteria questions, we see an increasing level of transparency, but with a median transparency of 86% in 2021, which is still too low. When there is such a high level of non-transparency across the rating evaluation questions, there is no reasonable expectation of how the product will collect and use personal information for revenue generation, including advertising purposes. We would expect to see better transparency for all of these questions. With the exception of indicating an effective date, which has 100% disclosure, we hope to see an additional 12-25% in disclosures across all of our other rating questions before we see a level of transparency necessary to make informed decisions regarding these critical practices.

Figure 15: Transparency analysis aggregated by question Rating questions

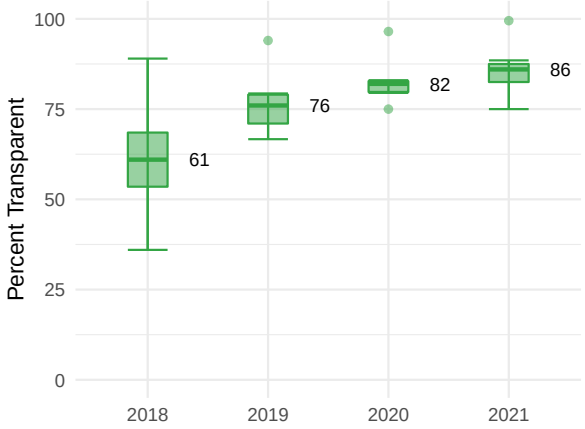


Table 10: Transparency analysis aggregated by question Rating questions descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	36	54	61	61	68	89
2019	67	71	76	77	79	94
2020	75	80	82	83	83	96
2021	75	82	86	86	88	100

As we shift our focus to product level transparency as seen in figure 16 and table 11, we see that overall products have increased transparency considerably since 2018 on our rating-related questions. Over 50% of products were 100% transparent across all rating criteria questions in 2021, as compared to 2018 when the median level of transparency for all products was only 71%. Due to this increase in transparency, any product below 86% transparency, meaning any product that is non-transparent on two or more of our seven rating criteria, is considered an extreme outlier in 2021 and is considered to be providing a level of transparency considerably lower than the industry standard. While this is a huge improvement for most products, the remaining products need to improve their privacy disclosures. Since 2018 we see nearly a 41% increase from 71% to 100% median transparency for products related to our rating criteria. Of note are considerable increases in disclosure regarding both Track Users and Data Profile. The passing of privacy legislation, especially the GDPR in 2018, increased scrutiny on creating automated data profiles for the purposes of advertising. Legislation regarding tracking users did not see notable changes until the CCPA was passed in 2019. We can only assume that a shift in societal awareness, including efforts such as our evaluation program and ratings indicating the importance and potential privacy riskiness of tracking users, are the motivators for this increasing transparency. Our rating system, including relatively straightforward labels such as "Fail", "Warning", and "Pass", serve to guide users to safer products even when they have little expertise or time to make an assessment, and attempt to communicate the shortcomings or causes for concern of products in just a few words.

Figure 16: Transparency analysis aggregated by product Rating questions

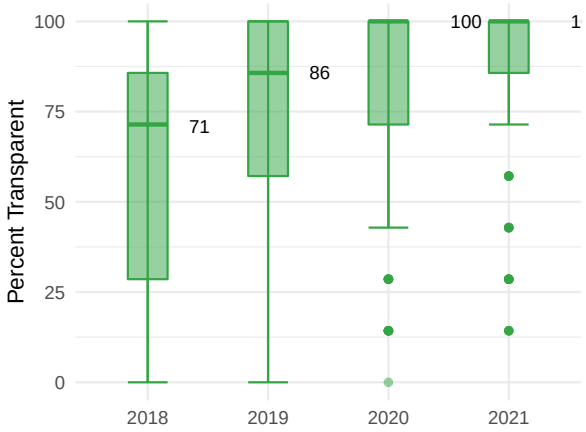


Table 11: Transparency analysis aggregated by product Rating questions descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	29	71	61	86	100
2019	0	57	86	77	100	100
2020	0	71	100	83	100	100
2021	14	86	100	86	100	100

Since 2018, surveys of consumers' views on privacy and risk indicate they are familiar with the practice of companies using their personal information to create detailed user profiles based on their traits and preferences for advertising purposes. However, the majority of respondents indicate that any benefits these practices may afford are not worth the added risks.[23] These risky practices are often referred to as "creepy," which is understood as an individual's subjective expectation of privacy that occurs when targeted advertising, tracking, profiling, or marketing communications take personalization a step too far and cross the line into perceived invasiveness. When third-party advertisements or marketing communications send messages that use an individual's information in a way that is too personal, or where the targeted messages appear in contexts that are too private, users may perceive the practice as creepy and decide that use of the product

[23] *See* Pew Research Center, Nov. 2019, *Key takeaways on Americans' views about privacy, surveillance and data-sharing*, https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing.

is not worth the risks. These "creepy" or creepy-enabling practices of targeted advertising, tracking, and profiling are included as evaluation questions in our rating criteria and likely serve to drive consumer awareness in the marketplace when choosing products that are more transparent about these issues and also disclose "better" privacy protecting practices. In response, companies have likely increased their transparency on these issues over the past four years in response to the changing privacy expectations of consumers on these "creepy" factors and how consumers differentiate and compare products on privacy.

Reading Statistics

Readability is a reader's ability to comprehend the language used in a document such as a privacy policy or terms of use. This is directly applicable to the ability of an individual to read and comprehend the privacy practices of a product's policies in order to make an informed decision to use the product themselves, or with their children and students. In calculating readability scores we use a combination of factors. For example, for reading time we use a custom algorithm based on a policy's text length with an average human reading speed of 1,000 characters per minute (cpm)[24] reduced by 10% for reading on a computer screen, and an additional 10% adjusted for reading technical legal language, arriving at a rough estimate of 800 cpm. To obtain the estimated minutes required to read a policy, we divide the text length in characters by 800 cpm. We calculate reading level by using the Flesch-Kincaid grade level algorithm.[25]

Reading Time

The reading time statistics shown in figure 17 and figure 18 consider just a product's privacy policy, which helps to normalize the analysis and minimize the disproportionate impact that products containing half a dozen or more supplemental policies in some cases would have. Note the change in y-axis

[24] *See* Trauzettel-Klosinski, Susanne; Dietz, Klaus (Aug. 2012). *Standardized Assessment of Reading Performance: The New International Reading Speed Texts IReST*. Investigative Ophthalmology & Visual Science. 53 (9): 5452–61. doi:10.1167/iovs.11-8284. PMID 22661485.

[25] *See* Kincaid J.P., Fishburne R.P. Jr., Rogers R.L., Chissom B.S. (Feb. 1975). *Derivation of new readability formulas (Automated Readability Index, Fog Count and Flesch Reading Ease Formula) for Navy enlisted personnel*. Research Branch Report 8-75, Millington, TN: Naval Technical Training, U. S. Naval Air Station, Memphis, TN.

Figure 17: Privacy policy only: Reading Time vs. Rating Score

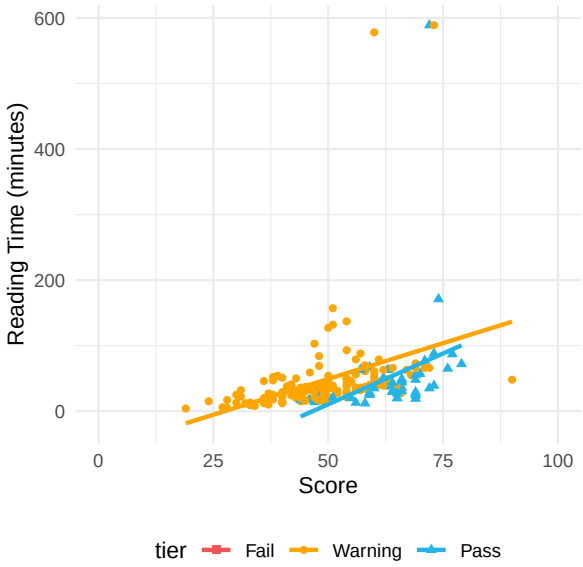
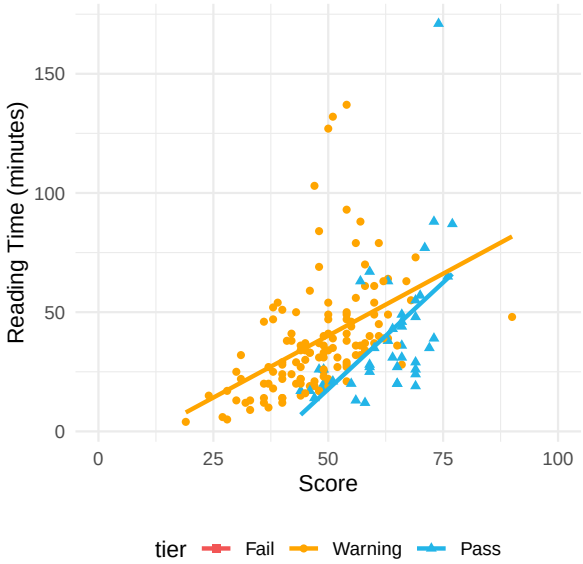


Figure 18: Privacy policy only: Reading Time vs. Rating Score products classified as big tech are suppressed from data.



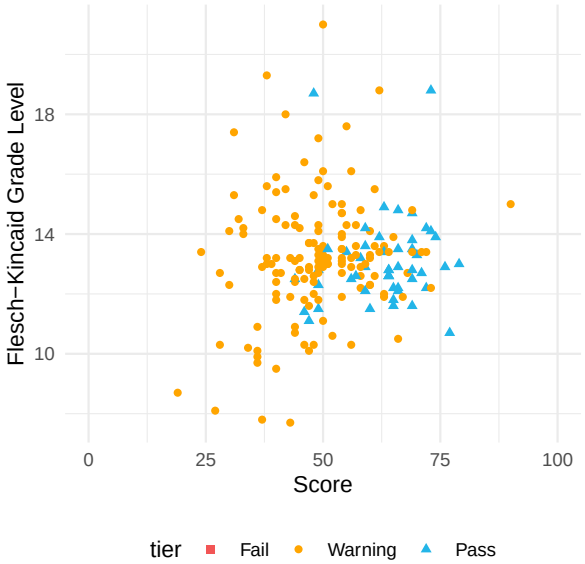
scale between the two figures as inclusion of products classified as big tech result in a y-axis scale nearly four times larger. The data indicates that the majority of products that received either a *Warning* or *Pass* rating, excluding big tech, have a privacy policy reading time of under 200 minutes as shown in figure 18. In general, *Pass* rating products receive a higher score in the same or shorter amount of reading time than products that received a *Warning* rating. This could be due to a variety of reasons, but disclosing "better" privacy protecting practices that apply to all uses of a product may be easier to explain in fewer words than "worse" privacy practices that apply to some users, but not others.

The reading time statistics charts are also filtered with big tech[26] in figure 17 and without big tech products in figure 18 because they skew the reading time scale. It is useful to note that big tech privacy policies or terms of use often cover a suite of products or sometimes all the products offered by the company, many of which might also be much older in age than products created by smaller companies. Therefore, with many more products' privacy practices to describe and potentially myriad features to discuss in a policy, it is expected that such policies could be considerably more time-consuming to read and are considered an extreme outlier in our reading time analysis.

After removing big tech from Figure 18, we notice that the majority of products require a user to spend over an hour just to read the product's privacy policy. In general *Pass* rating products are to the right of *Warning* products, implying that *Pass* products achieve a higher score in fewer words than warning products. While more text can and should lead to greater transparency in a policy, these transparency gains should not include unnecessarily lengthy or complicated text that further discourages people from learning about a company's practices. In general, *Pass* rating products receive a higher score in a shorter amount of reading time. Slightly longer policies that are simple, straightforward, and honest are preferable over short, vague, and dishonest policies. However, policies that are too long can make it too difficult to find information on all types of privacy practices both good and bad. People cannot be expected to read policies when the cost of doing so is too high for the hundreds of applications and services they use.[27] From these reading time results, we encourage companies to be aware of how long their policies are, and to work toward building policies that are organized, of manageable length, and informative in order to help consumers, parents, and educators make an informed decision on whether to use a product. Additional reading time charts are available in the Appendix that take into account not just the reading time of the product's privacy policy, but also all the additional policies a user is expected to read before using a product that include the terms of use, cookie policy, and other FAQs.

Reading Grade Level

Figure 19: Privacy policy only: Flesch-Kincaid Grade Level vs. Rating Score



When a policy is too difficult for the average person to understand, true transparency suffers even if a policy does describe "better" privacy practices. The average American adult reads at a middle-school level, or grades 6-8 in the Flesch-Kincaid grade levels.[28,29] From figure 19 we see that the vast majority

[26] The following products are considered "Big Tech" as they are owned by either Amazon, Apple, Facebook, Microsoft, or Google. These products are: Amazon Alexa, Amazon Kids+, Amazon Kindle, Amazon Prime Video, Apple School Manager, Apple Siri, AppleTV+, Facebook, GitHub, Goodreads, Google Assistant, Google Classroom, Google Family Link, iMessage, Instagram, iTunes U, Microsoft Office 365 Education, Microsoft Teams, Oculus for Facebook, Ring, Skype, WhatsApp Messenger, YouTube, and YouTube Kids.

[27] McDonald, A.M. and Cranor, L.F., *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society (2008), https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[28] *See* National Center for Education Statistics (NCES), *Fast Facts: Adult Literacy*, https://nces.ed.gov/fastfacts/display.asp?id=69.

[29] The Flesch-Kincaid readability test evaluates English text based on how hard the text is to understand based on word and sentence length.

of the policies in our dataset are well above an 8th-grade level. Most are clustered between grade levels 12-15 – an undergraduate university level of reading. A few of these products have policies that are above an undergraduate reading level, with some at a reading level over a completed master's degree (which would begin around Flesch-Kincaid grade level 16). This distribution is concerning, and certainly unfair if the goal is for the average American adult to realistically make an informed decision whether to use a product. As can be seen from the bottom right blue product in figure 19 which reflects a *Pass* rating with an approximate score over 75% and a reading level just barely over 10th-grade, it is possible for a company to earn a higher overall score and disclose "better" privacy practices in its privacy policy at a reading level that is more accessible.

Users of the same product will vary greatly in reading level, and policies should be accessible to as many users as possible (including in the Preferred Language of the user), not only to those who can interpret legal documents with expertise. Teenagers who access online services on their own should be just as able to read about and understand the privacy risks of using a product intended for their use as an adult with legal expertise. This can only be achieved by improving the readability of privacy policies – without compromising transparency for simplicity.

Score Distributions

The following sections illustrate the overall scores for both basic and full scores for popular kids' tech applications and services over the last four years.

Basic Scores

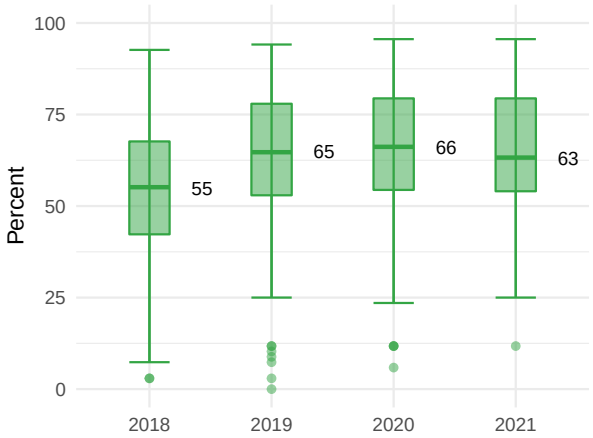
Among the applications and services evaluated, table 12 and figure 20 illustrate the basic score statistics over the past four years. From the analysis of basic evaluation questions, we determined a median score in 2021 of approximately 63%. This median is lower than expected, given that these applications 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 Ratings section, which are a varying subset of concern questions as seen in the Evaluation Concerns section. For example, basic evaluation questions include a subset of questions from all 10 privacy concerns, and to a varying degree of quality, a basic score may serve as a prediction of a full evaluation score, as discussed in the Basic and Full Score Comparison section. Lastly, the mean for basic scores is higher than their full score counterparts, and the minimum and maximum for basic scores is a wider range than as described in the Full Scores section below.

Table 12: Year-over-year results Basic Score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	3	42	55	54	68	93
2019	0	53	65	63	78	94
2020	6	54	66	65	79	96
2021	12	54	63	65	79	96

Compared to 2018, applications and services in 2021 indicate a 15% increase in the overall basic median score that indicates 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 Q1 and Q3 increasing by roughly 29% and 16% respectively. Lastly, because the industry has significantly improved its basic privacy practices since 2018 across all concerns, extreme outliers present and denoted with circles in 2020 have improved practices to be more consistent with industry norms.

Figure 20: Comparison of basic scores year-over-year results



Full Scores

Among the applications and services evaluated, table 13 and figure 21 illustrate full score statistics. We determined a median score in 2021 of approximately 53%. 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 across all Evaluation Concerns. Lastly, the median for full scores is lower than the median for basic scores 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 13: Year-over-year results Full Score descriptive statistics

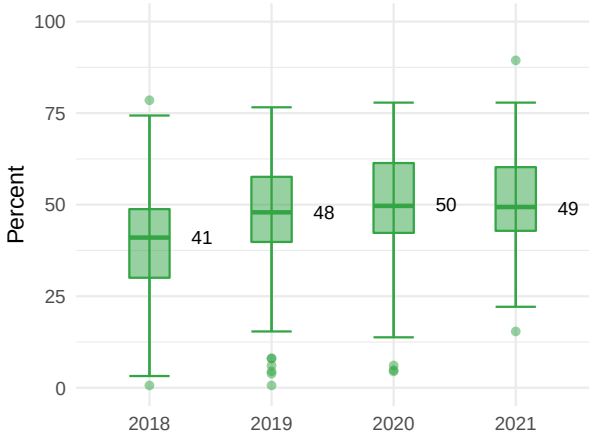
	Min.	Q1	Median	Mean	Q3	Max.
2018	1	30	41	39	49	79
2019	1	40	48	48	58	77
2020	4	42	50	51	61	78
2021	15	43	49	51	60	89

Compared to 2018, applications and services in 2021 show an approximate 20% increase in the full score median score, indicating more transparent and qualitatively "better" practices across a wide range of privacy practices. We see similar changes in the basic score, which is expected because the basic questions are a subset of the full evaluation questions and attempt to be a representative sample. In addition, since 2018, the industry has improved with greater transparency and "better" practices, as seen by Q1 and Q3 increasing by roughly 43% and 22% respectively. Lastly, because the industry has significantly improved its basic privacy practices since 2018, extreme outliers that are present and denoted with circles in 2020 have improved practices to be more consistent with industry norms.

Statute Scores

Each statute or regulation is associated with one or more evaluation questions in our evaluation process. As such, we can calculate scores for each statute or regulation using only those questions associated with the statute or regulation. Statute scores represent a more diverse range of privacy,

Figure 21: Comparison of full scores year-over-year results



safety, security, and compliance issues and reference more questions than Evaluation Concerns, which are focused narrowly on the most important 10 questions within a single category. Each specific statute or regulation score serves as a cross-contextual proxy indicating the likelihood of the application or service satisfying all of its compliance obligations. The following statute scores are focused on international privacy laws such as the GDPR, federal privacy laws such as COPPA and FERPA, and California state privacy laws such as the CCPA/CPRA, CalOPPA, SOPIPA, and Privacy of Pupil Records.

Table 14: 2021 statute score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
GDPR	20	50	60	59	71	95
COPPA	20	46	55	55	64	89
FERPA	17	36	49	48	58	90
CalOPPA	29	58	65	65	73	88
CPRA	17	51	59	60	71	90
SOPIPA	17	47	56	56	67	86
Pupil Records	7	37	60	57	77	100

However, a 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, such as for use with children or students. 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 that 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. Therefore, without additional context, statute scores can still provide valuable insight into how the most popular products used by children and students are disclosing their compliance obligations.

The following statute score analysis illustrates some of the most important privacy laws impacting children, students, parents, educators, and consumers.

General Data Protection Regulation (GDPR)

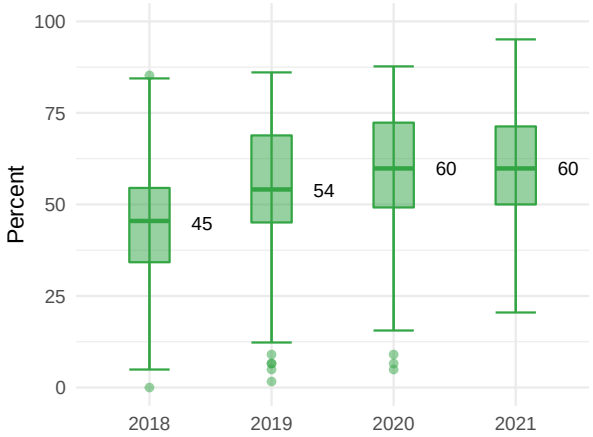
Figure 22 illustrates the statute scores for Europe's GDPR, which is an international privacy law that came into effect in 2018 with many reporting and compliance requirements for companies. The law provides European citizens with greater data rights and control over the collection, use, and disclosure 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 15 compares and summarizes the GDPR statute score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 15: Year-over-year results GDPR score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	34	45	44	55	85
2019	2	45	54	55	69	86
2020	5	49	60	59	72	88
2021	20	50	60	59	71	95

From the analysis of GDPR-related questions, which represent approximately 40% of all our questions, we determined a median score in 2021 of approximately 60%. This median score 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 every year since 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 22: Comparison of GDPR scores year-over-year results



Since 2020, GDPR median scores are stable but with higher minimum and maximum scores. Compared to 2018, applications and services evaluated in 2021 indicate a 33% 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 Q1 and Q3 increasing by roughly 47% and 29%

respectively. Lastly, because the industry has improved its GDPR compliance-related practices since 2018, we no longer see extreme outliers as denoted with circles in 2019 and 2020.

Children's Online Privacy Protection Act (COPPA)

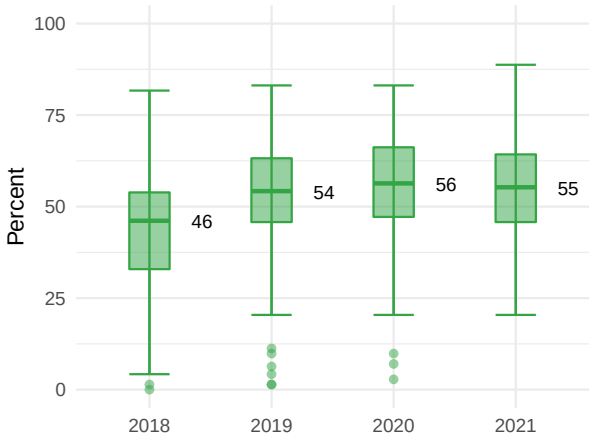
Figure 23 illustrates the statute scores for COPPA, which is a federal law with many requirements, including that the application or service must obtain parental consent before the collection or disclosure of personal information from children under 13 years of age.[30] Table 16 compares and summarizes 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) over the past four years.

Table 16: Year-over-year results COPPA score descriptive

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	33	46	44	54	82
2019	1	46	54	52	63	83
2020	3	47	56	55	66	83
2021	20	46	55	55	64	89

From the analysis of COPPA-related questions, which represent approximately 50% of all our questions, we determined a median in 2021 of approximately 55%. This median is lower than expected, given that these applications and services are intended for children and students. In addition, a majority of companies disclose qualitatively "better" practices in respect to children, which includes limiting the collection of personal information, and obtaining 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 a general-audience product and not intended for children under 13 years of age, but that still target children as the intended audience or would appeal to children under 13 years of age. A general-audience product may be considered to be directed at children if the product would appeal to children under 13 years of age. This 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.[31] Therefore, a general-audience product that collects personal information from users to teach them ABCs or basic numbers with animated cartoon characters would likely be a child-directed product and should disclose in their policy how they protect children's privacy. Comparatively, the COPPA minimum, median, mean, and maximum ranges are similar to the other 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 23: Comparison of Children's Online Privacy Protection Act (COPPA) scores year-over-year results



Since 2020, COPPA median scores remain stable at 55% with a higher maximum score. However, compared to 2018, applications and services evaluated in 2021 show a 20% increase in median COPPA scores, which indicates 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 2021 median of approximately 55% moving beyond the third quartile of the 2018 range of scores. Lastly, since COPPA compliance-related practices have improved since 2018,

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

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

we no longer see extreme outliers as denoted with circles in 2019 and 2020.

Family Educational Rights and Privacy Act (FERPA)

Figure 24 illustrates the statute scores for FERPA, which is a federal law with many requirements that protect the privacy of student education records.[32] Table 17 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) over the past four years.

Table 17: Year-over-year results FERPA score descriptive statistics

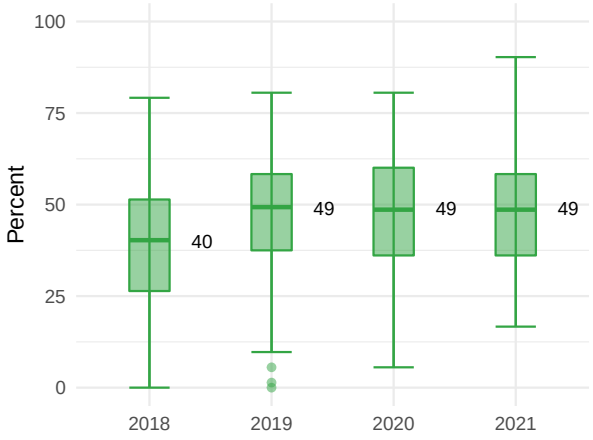
	Min.	Q1	Median	Mean	Q3	Max.
2018	0	26	40	39	51	79
2019	0	38	49	48	58	81
2020	6	36	49	48	60	81
2021	17	36	49	48	58	90

From the analysis of FERPA-related questions, we determined a median in 2021 of approximately 49%. This median is lower than expected, 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 institution 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 student data privacy agreement or 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 publicly available policies.

Since 2020, FERPA median scores have remained stable at 49%, but with a higher maximum score

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

Figure 24: Comparison of Family Educational Rights and Privacy Act (FERPA) scores year-over-year results



and higher minimum score. Compared to 2018, applications and services evaluated in 2021 show a 23% increase in FERPA median scores, indicating 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 38% and 14% respectively. Lastly, because the industry has improved its FERPA compliance-related practices since 2018, extreme outliers that were denoted with circles in 2019 have improved practices to be more consistent with industry norms. Among products evaluated over all four years, the trends are largely the same with an incrementally increasing median score since 2018.

California Privacy Rights Act (CPRA)

Figure 25 illustrates the statute scores for the California Privacy Rights Act (CPRA), which is a California state law that was passed in 2020 by ballot initiative.[33] The CPRA amended the previous California Consumer Privacy Act (CCPA) passed in 2019.[34] The CCPA included the following five core rights for consumers:

1. **The right to know** what personal information is collected, used, shared, or sold.

[33] *See* The California Privacy Rights Act of 2020, Proposition 24 in the November, 3 2020 General Election, https://thecpra.org.

[34] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.198.

2. **The right to opt out** of the sale of personal information. Children under the age of 16 must provide opt-in consent, with a parent or guardian providing consent for children under 13. Parents can also opt out on behalf of their children.
3. **The right to access, delete, and download** personal information.
4. **The right to non-discrimination** in terms of price or service when a consumer exercises a privacy right under the CCPA.
5. **A private right of action** for a data breach where reasonable security protections were not used by the company.

The CPRA, passed by ballot initiative, expanded the CCPA with many additional rights that include the following 10 core rights for consumers:

1. Created a new privacy right — the right to limit the use of sensitive personal information.
2. Created a new privacy right — the right to correct personal information.
3. Extended the right to opt out of sale to include opting out of the "sharing" of personal data.
4. Provided stronger safeguards for kids.
5. Created a new privacy right — the right to opt out of automated decision making and profiling.
6. Established a new enforcement agency — the California Privacy Protection Agency (CPPA).
7. Required businesses to provide data protection by default and perform data protection impact assessments.
8. Expanded the data breach private right of action.
9. Increased fines and enforcement ($2,500-$7,500).
10. Reduced the ability to weaken the privacy law in California.

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 examine: 1) the impact on CCPA-related statute scores before the CCPA went into effect in 2018; 2) scores after the CCPA was passed in 2019; 3) scores while the CCPA was in effect and the CPRA was passed in 2020; and 4) scores during 2021 and 2022 before the new CPRA will come into effect in January 2023. Table 18 compares and summarizes the CPRA statute score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 18: Year-over-year results CPRA score descriptive statistics

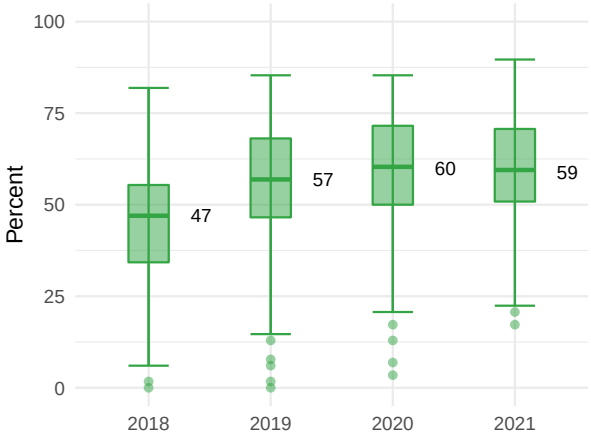
	Min.	Q1	Median	Mean	Q3	Max.
2018	0	34	47	45	55	82
2019	0	47	57	55	68	85
2020	3	50	60	59	72	85
2021	17	51	59	60	71	90

From the analysis of CPRA-related questions, which represent approximately 37% of all our evaluation questions, we determined a median score in 2021 of approximately 64%. These four-year median scores are retroactive, meaning that even though they encompass the compliance obligations of the future implementation of the CPRA before it goes into effect, our evaluation process is able to calculate scores as far back as 2018. This retroactive perspective is only possible because the new CPRA compliance obligations were already part of our larger full question Evaluation Framework.

However, the CPRA median score is lower than expected, given that these applications and services are required under the CCPA to provide notice to users of the ability to opt out of the sale of their data to third parties and disclose the ability for users to exercise their privacy rights. The low median score is likely the result of many factors that include a high percentage of non-transparency in a company's privacy policy with regard to many of the CCPA's and CPRA's requirements that also include questions reflected in our rating criteria. However, a majority of companies disclose qualitatively "better" practices in that they do not sell users' data to third parties and that the product provides privacy controls for users, such as the ability to access, modify, delete, and export their personal information any time through the product.

Since 2020 there has been no significant change in the median, mean, or maximum scores in 2021, which indicates that companies likely believe they

Figure 25: Comparison of California Privacy Rights Act (CPRA) scores year-over-year results



are in full compliance with the CCPA but do not feel they need to affirmatively disclose all compliance details. Comparatively, the CPRA's minimum, median, mean, and maximum ranges are similar to the other statute scores analyzed for this report, which may indicate that the majority of applications and services are only focusing on disclosing minimum compliance requirements. In addition, given that companies have had sufficient time to come into compliance with the CCPA's requirements established in 2019 and were required to respond to consumers' CCPA requests in 2020, companies need to update their policies to better reflect the CCPA's requirements because the forthcoming CPRA includes even more compliance obligations.

The CPRA is expected to come into effect in January 2023 with adoption of final regulations implementing the CPRA completed in July 2022. Enforcement by the new California Privacy Protection Agency (CPPA) will follow after the law comes into effect. Companies will be required to provide a clear and conspicuous link on the business's internet homepage, titled "Do Not Sell or Share My Personal Information," if they meet the statutory requirements of a covered "Business" and engage in the practice of selling or sharing personal information.[35] The median statute scores for compliance with the CPRA are already low, but it is expected that median scores will increase in 2022 with more transparency that discloses "worse" practices, as the definition of "sale" under the CCPA with our Sell Data evaluation question is expanded to include "sharing" a user's personal information with third parties for "cross-context behavioral advertising." This will implicate three of our existing evaluation questions: Third-party Tracking, Track Users, and Data Profile evaluation questions.

The CPRA defnes "**sell**," "selling," "sale," or "sold," as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a *third party for monetary or other valuable consideration*.[36] In addition, the CPRA introduces the new practice and definition of "**share**," "shared," or "sharing" which means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a *third party for cross-context behavioral advertising*, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.[37] Under the CPRA, **cross-context behavioral advertising** means the targeting of advertising to a consumer based on the consumer's *personal information* obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts.[38]

"**Personal information**" under the CPRA is included in the definition of "sale," "share," and "cross-context behavioral advertising" and includes inferences drawn from any personal information to create a *profile* about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.[39] "Profiling" means any form of automated processing of *personal information* to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior,

[35] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §1798.140(d)

[36] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ad)(1).

[37] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ah)(1).

[38] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(k).

[39] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(v)(1)(K).

location or movements.[40] Profiling under the CPRA is not considered a "Business Purpose" and personal information cannot be used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.[41]

However, the Behavioral Ads evaluation question is not included in the data sold analysis covered in the Multiple Privacy Practice Comparison section because the CPRA excludes the practice of behavioral ads in its definition of cross-context behavioral advertising, where behavioral advertising may use personal information only from the first-party business, distinctly-branded website, application, or service with which the consumer intentionally and directly interacts with. Our evaluation questions interpret targeted or behavioral ads that are displayed to the user on the first-party platform to be associated with the Behavioral Ads evaluation question. If personal information is shared with third parties to display targeted or behavioral ads to users on other third-party applications or services across the internet which the consumer does not intentionally interact with, we categorize that practice with our Track Users evaluation question.

Therefore, the new CPRA intersection of Third-party Tracking, Track Users, Data Profile and Sell Data will expand the definition of a company's selling practices. Since our evaluation process has always included these three questions, we can compare their historical practices since 2018 – as shown in figure 31 – and speculate about what a product's "selling" data practices will be after the CPRA becomes law. As indicated in our Sell Data evaluation question, as companies move from non-transparency about selling data to discussing statutory requirements related to selling data such as the CPRA's cross-context behavioral advertising, tracking, and profiling, they will most likely disclose "worse" practices for kids and families. For more information about the intersection of "better," "worse," or "unclear" practices of selling data with the additional variables of third-party tracking, tracking users, and data profiles, please see the Multiple Privacy Practice Comparison section.

[40] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(z), (aj).

[41] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(4).

California Online Privacy Protection Act (CalOPPA)

Figure 26 illustrates the statute scores for CalOPPA, which is a California state law with many requirements, including that an application or service that collects personally identifiable information through the internet about individual consumers residing in 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. Table 19 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).

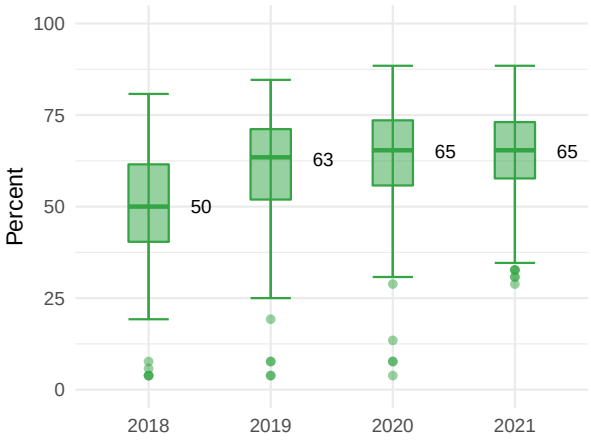
Table 19: Year-over-year results CalOPPA score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	4	40	50	49	62	81
2019	4	52	63	59	71	85
2020	4	56	65	63	74	88
2021	29	58	65	65	73	88

From the analysis of CalOPPA-related questions, we determined a median in 2021 of approximately 65%. 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 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 the most basic requirements of a privacy policy. If a company does not comply with CalOPPA's basic requirement that they post a publicly available privacy policy, they will receive our *Fail* rating.

Since 2020, CalOPPA statute median scores are stable with a higher minimum score. Compared to 2018, applications and services evaluated in 2021 for the statute of CalOPPA show an 30% increase

Figure 26: Comparison of California Online Privacy Protection Act (CalOPPA) scores year-over-year results



in median scores, indicating more transparent and qualitatively "better" practices related to the absolute 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 45% and 18% respectively. We still see some extreme outliers that are denoted with circles. However, because CalOPPA compliance-related practices have improved since 2018 the lower threshold for being an extreme outlier has improved considerably. Some of the products denoted as outliers in 2021 may not have been outliers in previous years, and are now considered to be underperforming relative to industry norms and should update their terms accordingly.

Student Online Personal Information Protection Act (SOPIPA)

Figure 27 illustrates the statute scores for SOPIPA, which is a California state law with many requirements that include applications or services primarily designed and marketed to K-12 schools and districts. These products must only use student information for educational purposes, and they must maintain reasonable security standards, and the product is prohibited from using student data for tracking, profiling, or behavioral advertising.[42] Table 20 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 20: Year-over-year SOPIPA score descriptive statistics

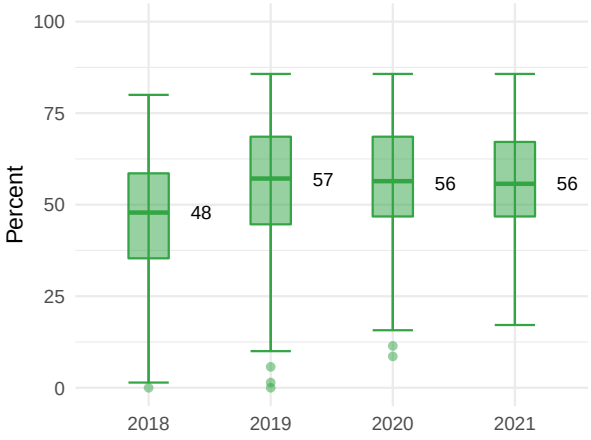
	Min.	Q1	Median	Mean	Q3	Max.
2018	0	35	48	46	59	80
2019	0	45	57	55	69	86
2020	9	47	56	56	69	86
2021	17	47	56	56	67	86

Since 2020 SOPIPA median scores are stable at 56% but with a higher minimum score. Compared to 2018, applications and services evaluated in 2021 indicate a 17% 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 Q1 and Q3 increasing by roughly 34% and 14% respectively. Lastly, because the industry has improved its SOPIPA compliance-related practices since 2018, extreme outliers that are denoted with circles in 2019 and were within the lower whisker in 2018 have improved practices to be more consistent with industry norms. However, these shifts may be due to products that were not evaluated since 2018 because they were either discontinued or no longer popular with students in K-12 schools and districts. Among products evaluated over all four years, the trends are largely the same with the different population demographics simply having different starting points since 2018.

However, this low SOPIPA median score may be attributable to incorrect assumptions by companies that SOPIPA does not apply to their applications and services. SOPIPA applies narrowly to specific companies–only products used primarily for K–12 school purposes and designed and marketed for K–12 school purposes. The California Privacy Rights Act (CPRA) fills in some of these gaps by requiring more transparency in privacy policies about what data is collected about students. This extra transparency can support educators to make a more informed decision about products they may want to use in the classroom, whether or not the product is designed and marketed for K–12 school purposes. In addition, the CPRA applies to any product that

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

Figure 27: Comparison of SOPIPA scores year-over-year results



sells users' data, regardless of whether it is intended for K-12 school purposes, so educators know that personal information of children cannot be sold without opt-in consent. Also, "education records" of students that are defined under FERPA are included in the CPRA's definition of "personal information," and therefore users over the age of 16 can opt out of the sale of their student data.

California Privacy of Pupil Records (Pupil Records)

Figure 28 illustrates the statute scores for California's Privacy of Pupil Records, which is a California state law with many requirements that authorizes a local educational agency (LEA)[43] to enter into a third-party contract with an application or service for the collection and use of pupil records that include digital storage, education software, and social media.[44] Table 21 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).

[43] A Local educational agency or LEA means a public board of education or other public authority legally organized within a state for either administrative control or direction of public elementary schools or secondary schools in a city, county, township, or school district.

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

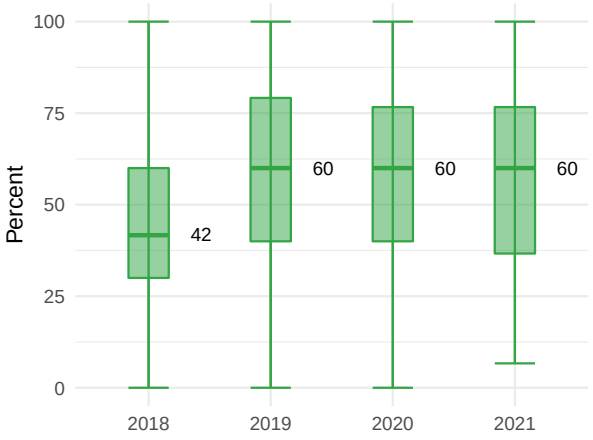
Table 21: Year-over-year results pupil records score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	30	42	45	60	100
2019	0	40	60	58	79	100
2020	0	40	60	59	77	100
2021	7	37	60	57	77	100

From the analysis of pupil records-related questions, we determined a median in 2021 of approximately 60%. 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 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. In addition, there appears to be no industry standard on disclosures related to the pupil records law because of the wide range of minimum and maximum scores of 7 and 100 respectively. Therefore, companies may assume that because the law requires a contractual relationship be established with the school or district and that the school, district, or faculty control the deployment of the application or service and administration of student accounts, that companies do not also need to disclose the contractual process or its requirements in their publicly available policies.

Since 2020 pupil records median statute scores are stable but with higher minimum scores. Compared to 2018, applications and services evaluated in 2021 show a 43% increase in pupil records median scores, indicating a significant increase in transparent and qualitatively "better" practices regarding the protection of students' personal information. In addition, since 2018 some products have improved their practices regarding contractual compliance with LEAs as seen by Q1 and Q3 increasing by 23% and 28% respectively. Lastly, this increase is not surprising because pupil records compliance requirements overlap with many other student data privacy laws such as FERPA and SOPIPA, and we saw similar increases in those respective statute

Figure 28: Comparison of California Privacy of Pupil Records scores year-over-year results



scores. Among products evaluated over all four years, the trends are largely the same with a 43% increase in both population demographics since 2018.

Analysis

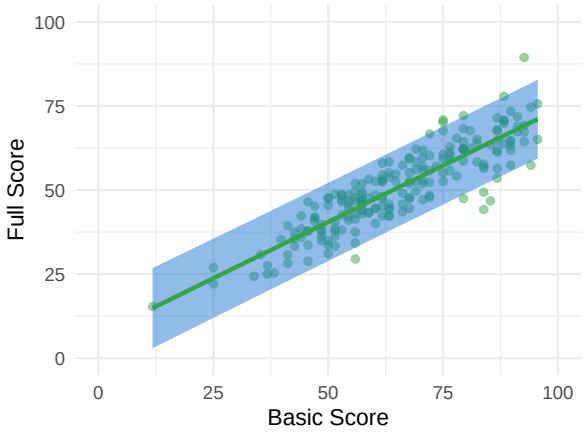
The following analysis seeks to understand the relationships and correlations between scores, ratings, and practices across multiple questions. First, when comparing a full score to a basic score, the intent is to identify whether the basic score is a reliable indicator of a full score. From our analysis, 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 industrywide.

Basic and Full Score Comparison

Figure 29 illustrates a comparison between the overall basic score and full score for all the applications and services evaluated for this report in 2021. 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 ±10 points and an r2 value greater than 0.7.

We 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 shaded area indicating the 95% prediction interval. In other words, the line and shaded 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 area. The r2 value is an indication of how well our linear model explains the variance in data. For the purposes of our basic to full score comparisons, r2 ≥ 0.7, and a prediction interval range less than 30 is considered a "reliable predictor." However, when r2 ≤ 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.

Figure 29: Comparison of 2021 comprehensive basic Scores and full Scores. The green line represents the linear regression defined by the equation $y = 7 + 0.67(x) \pm 12$, and $r^2 = 0.777$, where x is the basic score and y is the predicted full score. The shaded areas indicate the 95% prediction interval where we would expect 95% of the full scores to be given a specific basic score.



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. 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 fourth year of collecting 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, as our scoring methodology has a strong bias towards transparency over qualitative measures. 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 will fail to address the larger picture or more nuanced Evaluation Concerns as covered in our full evaluations.

Rating and Full Score Comparison

Figure 30 illustrates the rating and full score statistics among the 200 popular applications and services evaluated. Table 22 summarizes the ratings 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).

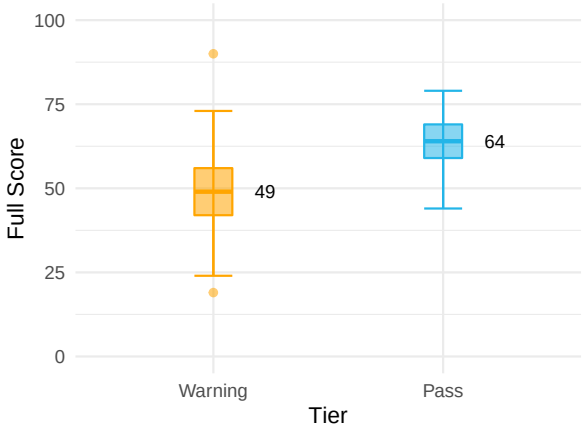
Table 22: 2021 rating score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
Warning	19	42	49	49	56	90
Pass	44	59	64	63	69	79

From the analysis of the ratings and their respective full scores for the applications or services evaluated in 2021, as described in the Evaluation Ratings section, we determined a median of the blue *Pass* rating of approximately 64%. In addition, we determined a median of the orange Warning rating of approximately 49%, and no products evaluated were represented in the Fail rating.

The *Pass* median score is lower than expected, given that these applications and services are intended to be used by children and students. Companies in this rating 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.

Figure 30: Distribution of 2021 scores relative to their respective ratings



This lower score is likely the result of companies focusing exclusively on disclosing qualitatively "better" practices to ensure they are not in the *Warning* rating, but failing to disclose additional privacy and security practices across all of the evaluation questions resulting in a lower overall score. Interestingly, the *Pass* lower quartile has roughly the same spread as the *Warning* interquartile range, and the *Pass* minimum is within the *Warning* second quartile. As figure 30 illustrates, there are many applications and services with a *Pass* rating that disclose qualitatively "better" practices, but have less robust policies and earn the same full score as many products with a *Warning* rating. In addition to disclosing "better" practices regarding selling data, advertising and third-party data use, products receiving a *Pass* rating tend to be more transparent than warning products in other privacy concerns as well, and thus typically achieve higher scores than most products earning a Warning rating.

Moreover, approximately 75% of the products earning a *Warning* rating have full scores that fall within the range of scores earned by products in the rating *Pass*. However, 100% of products earning a *Pass* rating achieve scores at or higher than approximately 25% of products receiving a *Warning* rating. When the Common Sense Privacy Program started evaluating products, we found that transparency among the most popular products was very poor and we were unable to make an informed assessment about the privacy practices of products across many areas. Therefore, we focused on a scoring and rating methodology that encouraged transparency to balance the interests of companies with advocating for more information about a product's privacy practices in order to enable users to make an informed

decision. Creating a high-level scoring methodology to summarize the complex landscape of privacy and the differing contexts in which applications or services may be used is quite challenging. One individual data point or score is typically not enough information to determine whether or not an application is safe to use in a particular context. The full score overlap between the two ratings 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 ratings. As described in our Evaluation Concerns section, our evaluation process also provides additional details about a product beyond a rating 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.

Multiple Privacy Practice Comparison

The following multiple privacy practice comparison explores the privacy practices of a product at the intersection of multiple issues used in our rating criteria. For example, consider a product that discloses they sell data to third parties, and also that the product is intended for children or students. A product is considered "intended for children" when the company's policies transparently disclose either the product is intended for children, or users may be under the age of 13 years old, or that COPPA applies to the product because an user may be a child. The Sankey charts below aim to help visualize the complex and sometimes problematic combination of practices engaged in by products that are used by children or students.

Data Sold: "better"

The practice of monetizing users' personal information by selling data to third parties is a complex and evolving privacy issue. The passage of recent state consumer privacy protection laws enable consumers to opt-out of a company selling their data, but the definition of what selling data means for companies is expected to expand to include the use of data monetization practices such as third-party tracking and profiling technologies that will significantly impact the industry. Table 23 indicates for the 143 companies that disclose in their policies that they do not Sell Data to third parties, labelled as "better," whether they also disclose problematic privacy practices that could be considered monetizing users' data for monetary or other valuable consideration, labelled as "worse." Three additional rating criteria questions are filtered below: the use of Third-party Tracking technologies, Tracking Users on other applications and services across the internet, and creating Data Profiles for advertising purposes.

Table 23: Data Sold better vs. Third-Party Tracking vs. Track Users vs. Data Profile 2021. Row coloring indicates the expected "Data Sold" disclosure after the CPRA comes into effect. Blue indicates a "better" disclosure, orange indicates "unclear" but likely "worse", and red indicates "worse"

Third-Party Tracking	Track Users	Data Profile	count
better	better	better	55
unclear	unclear	unclear	11
unclear	unclear	better	3
unclear	better	unclear	1
unclear	better	better	1
better	unclear	unclear	1
better	better	unclear	1
worse	worse	worse	38
worse	worse	unclear	11
worse	worse	better	6
worse	unclear	worse	2
worse	unclear	unclear	5
worse	unclear	better	1
worse	better	worse	1
worse	better	unclear	3
worse	better	better	1
unclear	worse	worse	1
better	worse	better	1

We are encouraged that 38% (55/143) of the 143 products that disclose they do not sell a user's data, also disclose they do not use third-party tracking technologies, do not track users across the internet, and do not create data profiles for advertising purposes. However, 49% (70/143) of companies that disclose they do not sell data still engage in additional monetization practices, Third-Party Tracking "worse," Track Users "worse," or Data Profile "worse" that would likely be considered selling data with cross-context behavioral advertising under the CPRA.[45] In addition, the approximate 13% (18/143)

[45] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(k).

of companies that disclose that they do not sell users' data but are non-transparent about the use of third-party tracking technologies, tracking users, or data profiles are assumed to engage in "worse" practices. This assumption is based on the Sell Data evaluation question that indicates that over the long term when companies update their policies to disclose whether they sell data, those disclosures are more likely qualitatively "worse."

Another important factor to consider is that the CPRA is expected to go into effect in January 2023. Companies will be required under the CPRA to incorporate the use of third-party tracking technologies, tracking users across the internet, and creating data profiles for advertising purposes into their definition of "selling" or "sharing" a user's data for advertising purposes in exchange for monetary value or other valuable consideration. As a result, our data indicates there could be a significant shift in the industry with the percentage of companies that change their policies to disclose they now sell users' data under the CPRA. In 2021, only the Sell Data evaluation question is used to indicate that 14% of products explicitly disclose they sell users' data to third parties, with another 14% non-transparent or "unclear" on the issue.

The changes related to the CPRA are expected to be a monumental shift in the industry in 2022, with companies scrambling to update their policies with more transparency to meet the January 2023 deadline. The industry may shift their practices in response to the CPRA and stop Third-party tracking, Track Users, and Data Profile practices on their products to be able to continue to say in their policy that they "do not sell data." Companies that already say they Sell Data are not likely to change their practices or policies regarding the sale of data, but they may increase their transparency on the use of tracking technologies and data profiles for advertising purposes that will be considered a sale under the CPRA.

The percentage of companies with secondary practices that will also likely be considered selling data under the new CPRA is expected to increase significantly from 14% to at least 58%.

However, the industry will more likely increase transparency and continue to use tracking technologies in their products to monetize user data, but update their privacy policy to say they now Sell Data and also use tracking technologies and data profiles for advertising purposes. When regulations implementing the CPRA are finalized in 2022, it is likely the privacy practice disclosures of the brands and products consumers use every day will change overnight. When consumers learn that the companies and brands they trust changed their privacy policies from "we don't sell any data" to "now we sell your data" to reflect their already existing practices, there will likely be product reputational damage paired with consumer confusion for the change in practices and lost revenue for companies. Consumers are increasingly concerned about their privacy and fundamentally already understand that "selling data" means companies make money from various methods that include tracking their activities on the product and selling their data to third-party companies for advertising purposes.[46]

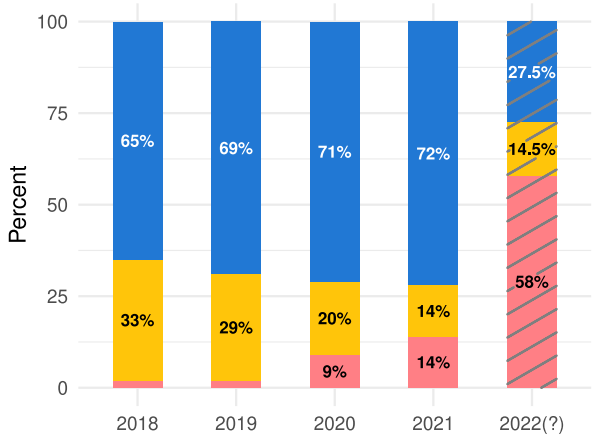
The majority of companies that say they do not sell users' data to third parties, but received a Warning rating as a result of "worse" or "unclear" tracking related practices and creating data profiles for advertising purposes, will likely change their policy in 2022 to say they now sell data to third parties.

Similarly to how companies claimed the definition of "sell" under the CCPA was unclear in their policies, or that the industry cannot agree on how to respond to DoNotTrack Response requests, we also expect that companies may blame the passage of multiple state consumer privacy laws and regulatory confusion for their policy change that says they now sell data. However, there may be pushback from consumers against companies that say they now sell data, but disagree with what selling means, in an attempt to redirect blame to confusing privacy laws. The CPRA's expansion may actually align more closely with consumers' expectations and understanding of what selling data means and how companies use various technologies and methods to actually make money from their data.

[46] *See* Pew Research Center, Nov. 2019, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf.

Lastly, companies with policies that are non-transparent on the issue of selling data, and are also non-transparent on the use of third-party tracking, tracking users, or data profiles, are presumed to likely be selling data as indicated in figure 31 supported by our long-term research on this issue. Including the non-transparent or "unclear" products would increase the portion of applications or services that disclose they sell data under the CPRA from 58% to 73%. For more background details on privacy laws that impact the practice of selling data, please see the California Privacy Rights Act (CPRA) section.

Figure 31: Speculative Data Sold responses in 2022 if industry does not change practices based on current responses to Data Sold, Third-Party Tracking, Track Users, and Data Profile



Data Sold: "worse"

Table 24 indicates for the 29 products that disclose the qualitatively "worse" practice that they do Sell Data to third parties, does the company also disclose privacy practices that could be considered monetizing users' data for monetary or other valuable consideration under the CPRA, labelled as "worse" in the table. Three additional rating criteria questions are filtered below: Third-party Tracking technologies, Tracking Users on other applications and services across the internet, and creating Data Profiles for advertising purposes.

Table 24: Data Sold worse vs. Third-Party Tracking vs. Track Users vs. Data Profile 2021. Row coloring indicates the expected "Data Sold" disclosure after the CPRA comes into effect. Blue indicates a "better" disclosure, orange indicates "unclear" but likely "worse", and red indicates "worse"

Third-Party Tracking	Track Users	Data Profile	count
worse	worse	worse	25
worse	unclear	unclear	1
unclear	unclear	unclear	1
better	better	unclear	1
better	better	better	1

It is not surprising that 89% (26 /29) of the 29 companies that disclose they do sell a user's data also disclose they use third-party tracking technologies, track users across the internet , or create data profiles for advertising purposes. These additional monetization practices will be considered selling data with cross-context behavioral advertising under the CPRA. In addition, companies that say they sell data but are "unclear" about the use of third-party tracking technologies, tracking users, or data profiles are assumed to also engage in these "worse" practices.

Data Sold: "unclear"

Table 25 indicates for the 28 products that do not disclose either a qualitatively "better" or "worse" practice that they do not or do Sell Data to third parties, does the company also disclose privacy practices that could be considered monetizing users' data for monetary or other valuable consideration under the CPRA, labelled as "worse." Three additional rating criteria questions are filtered below: Third-party Tracking technologies, Tracking Users on other applications and services across the internet, and creating Data Profiles for advertising purposes.

Table 25: Data Sold unclear vs. Third-Party Tracking vs. Track Users vs. Data Profile 2021. Row coloring indicates the expected "Data Sold" disclosure after the CPRA comes into effect. Blue indicates a "better" disclosure, orange indicates "unclear" but likely "worse", and red indicates "worse"

Third-Party Tracking	Track Users	Data Profile	count
unclear	unclear	unclear	8
unclear	better	unclear	1
better	better	unclear	1
better	better	better	1
worse	worse	worse	10
worse	worse	unclear	3
worse	worse	better	1
worse	unclear	worse	2
worse	unclear	unclear	1

Approximately 61% (17 /28) of the 28 products that do not disclose whether they sell a user's data, also disclose they use third-party tracking technologies, track users across the internet, or create data profiles for advertising purposes. Companies may not consider the transparent disclosure of third-party tracking or advertising practices the same practice as selling a user's personal information to third parties. Companies may think they are simply making money by providing *access* to their product for third parties with their users' automatically collected information. There is also likely a higher awareness among consumers about the practice of selling data, which may indicate why companies remain "unclear" or non-transparent on the issue, but still disclose the practice of using third-party tracking technologies to track users on other sites and services across the internet. As discussed, these additional monetization practices will also be considered selling data with cross-context behavioral advertising under the CPRA. In addition, companies that do not say whether they sell data and are also "unclear" or non-transparent about the use of third-party tracking technologies, tracking users, and data profiles are assumed to also engage in these "worse" practices.

Children Intended: Data Sold

Figure 32 and table 26 explore disclosures for all 200 products related to Children Intended and Selling Data of users to third parties. Nearly all of the products evaluated disclose whether or not children are intended users. Approximately 76% (96/127) of the 127 products intended for kids also indicate that data collected is not sold to third parties. We hope and expect that the ratio of selling data "better" practices will be higher for the 96 products that disclose they are intended for children (approximately 76%) than for those products that are not intended for children (approximately 64%) (40/62).

In 2021, more than six times the number of products intended for children disclosed that they did not sell children's data than those that disclosed they do sell data –which may include selling adult users' data, but not children's data if using a child profile.

For the 62 services not intended for children, we noticed nearly 3 times the number of services having "better" practices (40) than "worse" practices (14), but we still find this ratio to be a positive trend for kids, because kids are still using these products that have "better" privacy practices. However, for products where the policies disclose children are the intended audience and also disclose data is sold to third parties, it may be the case that these companies are limiting the sale of data to only data from adult users of the product when they have Actual Knowledge that the user is an adult, which we still classify as selling data as indicated in the Selective Privacy section.

Figure 32: Children Intended compared to Data Sold

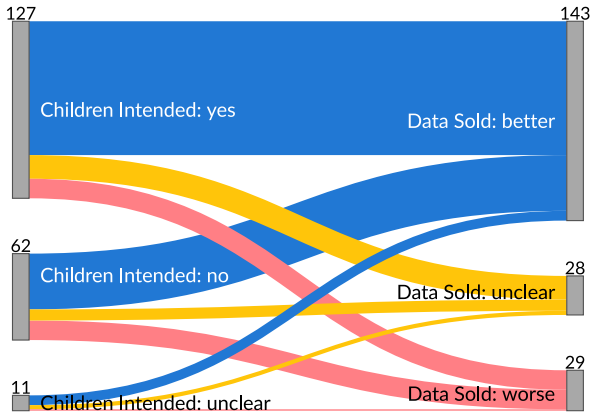


Table 26: Children Intended vs Data Sold 2021

Children Intended	Data Sold	count
no	worse	14
no	unclear	8
no	better	40
unclear	worse	1
unclear	unclear	3
unclear	better	7
yes	worse	14
yes	unclear	17
yes	better	96

Children Intended: Third-party Marketing

Figure 33 and table 27 explore disclosures for all 200 products related to Children Intended and Third-party Marketing communications. Nearly all of the products evaluated disclose whether or not children are the intended users. Of the 127 products intended for children, approximately 37% (47/127) indicate that data collected from users of the product may be used to send third-party marketing communications to users, vs. approximately 48% (61/127) that do not send third-party marketing communications to users.

In 2021 the data indicates that approximately half of the products intended for children have either "unclear" or "worse" practices that allow for sending third-party marketing communications to kids.

Regardless of whether or not products are intended for children, we find unfortunately high percentages of products engaging in third-party marketing, although we find this slightly less concerning for those products that are not intended for children due to the products' declared general-audience purpose. Recall that the products not intended for children may contain commonly used services that are intended for adults and are not subject to child or student-specific privacy laws. The dramatic increase in online learning in spring 2020 due to the COVID-19 pandemic gave rise to the increased use by children and teens of many products for education at home that were not intended for educational purposes or use by children; however, companies should still put in place "better" privacy practices if they have Actual Knowledge that children or students are using the product.

Figure 33: Children Intended compared to Third-Party Marketing

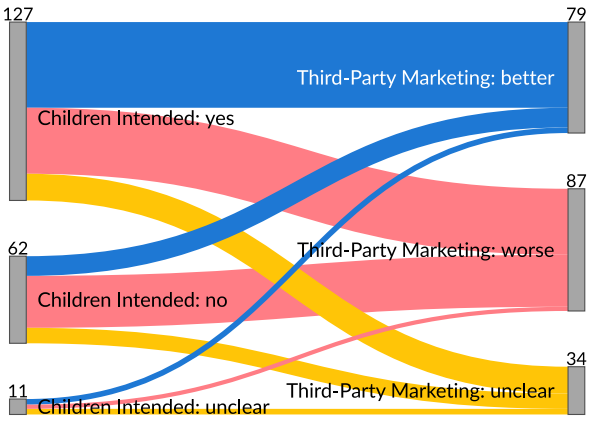


Table 27: Children Intended vs. Third-Party Marketing 2021

Children Intended	Third-Party Marketing	count
no	worse	37
no	unclear	11
no	better	14
unclear	worse	3
unclear	unclear	4
unclear	better	4
yes	worse	47
yes	unclear	19
yes	better	61

Children Intended: Behavioral Ads

Figure 34 and table 28 indicate that given a company's policies disclose the product is intended for children, does the company also disclose the qualitatively "worse" practice that they display targeted or Behavioral Ads. The data indicates approximately 95% transparency for products ((127 + 62) / 200) that explicitly disclose whether or not children are intended users. For the 127 products intended for children, this transparency results in a split between "better" 52% (66/127) and "worse" 37% (47/127) practices, which indicate that data collected from users of the product may be used to target advertising to kids. In addition, for the 62 products not intended for children, the data indicates that

nearly 60% (37/62) of products have "worse" practices that use personal information to display targeted advertising to other users of the product, who could include consumers, parents, and educators.

In 2021, a higher number of products intended for children disclosed that they did not display targeted ads than did those that disclosed they display targeted ads –which may include displaying ads to adult users but not to children who are using a child profile.

However, for products where the policies disclose children are the intended audience and also display targeted advertising, it may be the case that these companies are limiting display of targeted ads to only adult users of the product. Mixed-audience products often allow children to create accounts without indicating their age with age-gates or other birth date verification systems – which would inadvertently expose children to targeted advertising practices unless the company has Actual Knowledge the user is a child under 13 years of age and prevents displaying behavioral advertising to child users of their product.

Figure 34: Children Intended compared to Behavioral Ads

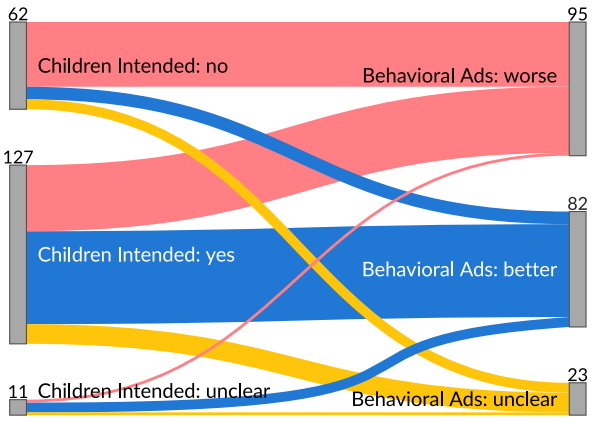


Table 28: Children Intended vs. Behavioral Ads 2021

Children Intended	Behavioral Ads	count
no	worse	46
no	unclear	7
no	better	9
unclear	worse	2
unclear	unclear	2
unclear	better	7
yes	worse	47
yes	unclear	14
yes	better	66

Children Intended: Third-party Tracking

Figure 35 and table 29 indicate that given a company's policies disclose the product is intended for children, does the company also disclose the qualitatively "worse" practice that they use Third-party Tracking technologies for advertising purposes. The data indicates approximately 95% transparency for products that explicitly disclose whether or not children are intended users. For products intended for children, this transparency results in a split between approximately 41% (52/127) "better" and approximately 46% (58/127) "worse" practices, which indicate that data collected from users of the product may be used to track children for advertising purposes. In addition, for the 62 products not intended for children, the data indicates that approximately 77% (48/62) have "worse" practices that use third-party tracking technologies such as cookies, unique identifiers, or fingerprinting techniques for advertising purposes.

In 2021, roughly the same number of products intended for children disclosed that they track users with third-party technologies as those that disclosed they do not track users –which may include tracking adult users but not children who are using a child profile.

For products with policies that disclose children are the intended audience and also track users, it may be the case that these companies are limiting tracking technologies to only adult users of the product. Products often allow children to create accounts

without indicating their age with age-gates or other birth date verification systems, which would inadvertently expose children to "worse" tracking practices until the company has actual knowledge the user is a child under 13 years of age.

Figure 35: Children Intended compared to Third-Party Tracking

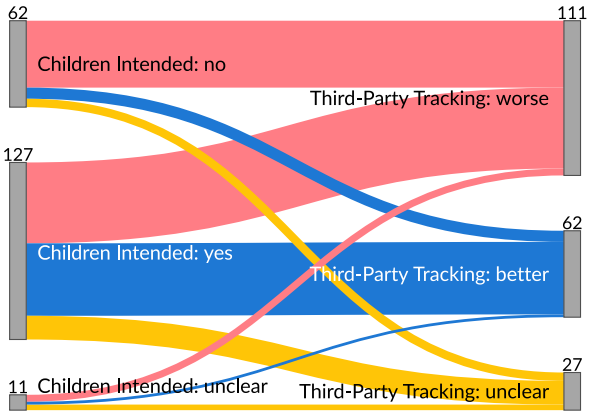


Table 29: Children Intended vs. Third-Party Tracking 2021

Children Intended	Third-Party Tracking	count
no	worse	48
no	unclear	6
no	better	8
unclear	worse	5
unclear	unclear	4
unclear	better	2
yes	worse	58
yes	unclear	17
yes	better	52

Children Intended: Track Users

Figure 36 and table 30 indicate that given a company's policies disclose the product is intended for children, does the company also disclose the qualitatively "worse" practice that they Track Users on other applications and services across the internet for advertising purposes. The data indicates approximately 95% transparency for products that explicitly disclose whether or not children are intended users. For the 127 products intended for children, this transparency results in a split between approximately 43% (55/127) "better" and approximately 39% (50/127) "worse" practices, which indicate that data collected from users of the product may be used to track children across other devices and applications for advertising purposes. In addition, for the 62 products not intended for children, the data indicates approximately 68% (42/62) of products have "worse" practices that track users with various technologies such as cookies, unique identifiers, or fingerprinting techniques across the internet which could include tracking consumers, parents, and educators.

In 2021, roughly the same number of products intended for children disclosed that they track users on other devices, applications, and services across the internet as those that disclosed they do not track users –which may include tracking adult users but not children who are using a child profile.

For products where the policies disclose children are the intended audience and also track users, it may be the case that these companies are limiting tracking technologies to only adult users of the product. Products often allow children to create accounts without indicating their age with age-gates or other age verification systems which would inadvertently expose children to "worse" tracking practices until the company has actual knowledge the user is a child under 13 years of age.

Figure 36: Children Intended compared to Track Users

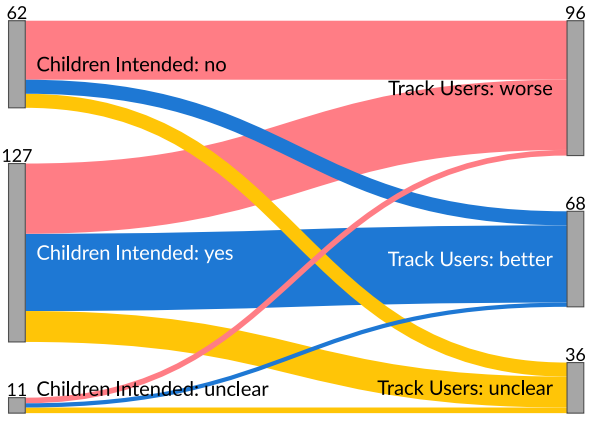


Table 30: Children Intended vs. Track Users 2021

Children Intended	Track Users	count
no	worse	42
no	unclear	10
no	better	10
unclear	worse	4
unclear	unclear	4
unclear	better	3
yes	worse	50
yes	unclear	22
yes	better	55

Children Intended: Data Profile

Figure 37 and table 31 indicate that given a company's policies disclose the product is intended for children, does the company also disclose the qualitatively "worse" practice that they amass a Data Profile about a user for advertising purposes. The data indicates approximately 95% transparency for products that explicitly disclose whether or not children are intended users. For the 127 products intended for children, this transparency results in a three-way split between 24% (30/127) "unclear," 46% (58/127) "better," and 31% (39/127) "worse" practices, which indicate that data collected from users of the product may be used to create a profile for data brokers or advertising purposes on other applications and services across the internet. In addition, for the products not intended for children, the data indicates approximately 58% (36/62) have "worse" practices that data collected from users of the product are used to create a profile.

In 2021, a higher number of products intended for children were both "unclear" and disclosed that they create data profiles of users for advertising purposes on other devices, applications, and services across the internet, than the number of those that disclosed they do not create data profiles.

However, for products where the policies disclose children are the intended audience and also create data profiles of users, it may be the case that these companies are limiting data profile creation to only adult users of the product. Products often allow children to create accounts without indicating their age with age-gates or other age verification systems which would inadvertently expose children to "worse" data profile practices unless the company has actual knowledge the user is a child under 13 years of age.

Figure 37: Children Intended compared to Data Profile

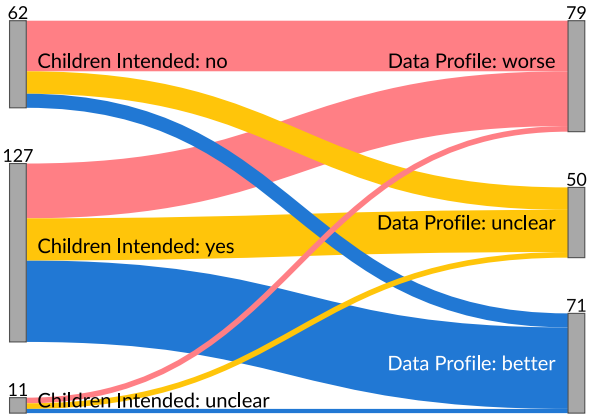


Table 31: Children Intended vs. Data Profile 2021

Children Intended	Data Profile	count
no	worse	36
no	unclear	16
no	better	10
unclear	worse	4
unclear	unclear	4
unclear	better	3
yes	worse	39
yes	unclear	30
yes	better	58

School Purpose: Students Intended

Figure 38 and table 32 indicate that given a company's policies disclose the product is primarily intended for school use in K-12 classrooms, does the company also disclose the product is intended for use by students. This is a nuanced difference under SOPIPA, but products can be intended for a general or mixed audience that includes students while not being primarily marketed to schools and districts. An example would be a phonics app designed for parent use to help their students with language learning in the home but that is not primarily marketed to schools and districts. Also, just because a product is

non-transparent or "unclear" as to whether or not students are an intended audience does not mean that the product is not used in schools.

In 2021, approximately 41% (82/200) of products are "unclear" on whether or not student use is intended, and also "unclear" on whether the product is intended for a school purpose.

This low percentage may be the result of our population shift since 2018 that included more products classified as kids' tech than products for use in the classroom, because kids' tech products are intended for a general or mixed audience that includes children under 13 years of age and companies may not be aware students are using their products. It is surprising that 7 products that are "unclear" about whether they are intended for students still disclose they are primarily used in K-12 schools and districts for a school purpose. It is possible that companies remain "unclear" or non-transparent about whether students are intended users or whether the product is primarily used for a school purpose because the companies always negotiate with schools and districts to put in place additional student data privacy agreements that clarify these issues. Alternatively, these products may be intended for administrative use. In addition, the majority of products evaluated, 54% (107/200), disclose they are intended for students, but slightly less than 50% (99/200) disclose they are primarily used for a school purpose. Companies need to more clearly define their intended audience and specify if the product may be used by students, which requires additional student data privacy protections be put in place in the product's privacy policy to protect any students using the product for an educational purpose.

Figure 38: School Purpose compared to Students Intended

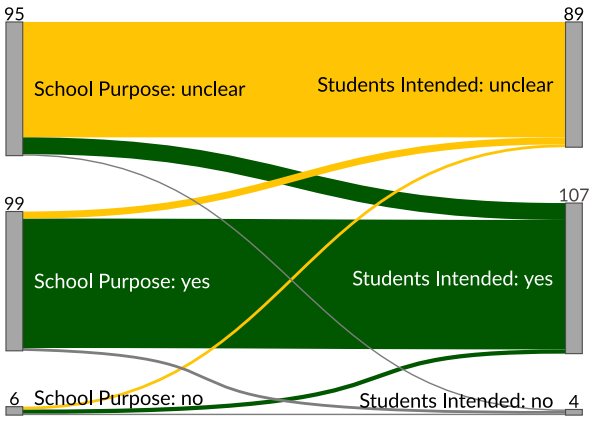


Table 32: School Purpose versus Students Intended 2021

School Purpose	Students Intended	count
no	no	1
no	unclear	2
no	yes	3
unclear	no	1
unclear	unclear	82
unclear	yes	12
yes	no	2
yes	unclear	5
yes	yes	92

Students Intended: Behavioral Ads

Figure 39 and table 33 indicate that given a company's policies disclose the product is intended for students, does the company also disclose the qualitatively "worse" practice that they display targeted or Behavioral Ads. The data indicates that approximately 48% (95/200) of all products evaluated disclose they engage in the "worse" practice of using personal information from users to serve targeted or Behavioral Ads whether or not students are intended. When students are intended users of the product, approximately 35% (37/107) of products disclosed "worse" practices and 11% (12/107) of products were "unclear" about whether behavioral advertising was displayed to users. Lastly, if you also include products that are "unclear" about whether targeted advertisements are displayed to students, that means a total of 46% ((37 + 12)/107) of products have the potential to serve ads to students

based on their personal information. These findings are surprising given that displaying targeted advertisements to students using personal information is a prohibited practice under federal and state student data privacy laws. However, this "worse" practice may not be illegal under student data privacy laws if targeted advertisements are only shown to adult users of the product such as parents or educators, or the company displays targeted advertisements to all users of the product unless they have Actual Knowledge that the user is a child under the age of 13 or a student.

In 2021, almost half of products that disclosed they are intended for students also disclosed "worse" practices or were "unclear" about serving targeted or behavioral advertisements.

Figure 39: Students Intended compared to Behavioral Ads

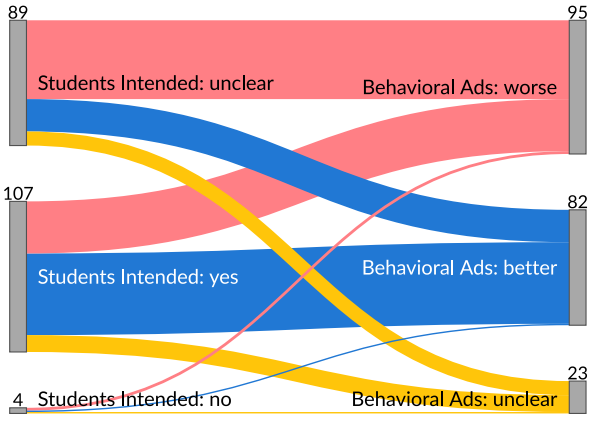


Table 33: Students Intended vs. Behavioral Ads 2021

Students Intended	Behavioral Ads	count
no	worse	2
no	unclear	1
no	better	1
unclear	worse	56
unclear	unclear	10
unclear	better	23
yes	worse	37
yes	unclear	12
yes	better	58

Students Intended: Traditional Ads

Figure 40 and table 34 indicate that given a company's policies disclose the product is intended for students, does the company also disclose the qualitatively "worse" practice that they display Traditional Ads. Traditional or contextual advertising in schools (ads served without the use of personal information) has been a long accepted practice in most schools. Selling ads for display in yearbooks or allowing a soft drink company to purchase a scoreboard for the athletic program to display their logo or product to students is a common practice. However, this is very different from the use of behavioral or targeted advertising that uses personal information from a student to display a personalized advertisement.

This might help explain the fact that 45% (48/107) of products that indicated they are intended for students engage in the "worse" practice of serving traditional or contextual ads to users. Only 35% (38/107) of products intended for students disclosed they did not display any contextual or traditional advertisements.

In 2021, almost half of all products that disclose they are intended for students for educational purposes also monetize the application or service through the use of contextual advertising.

Figure 40: Students Intended compared to Traditional Ads

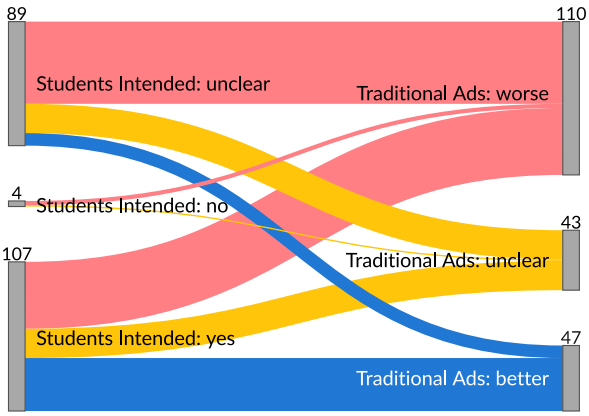


Table 34: Students Intended vs. Traditional Ads 2021

Students Intended	Traditional Ads	count
no	worse	3
no	unclear	1
unclear	worse	59
unclear	unclear	21
unclear	better	9
yes	worse	48
yes	unclear	21
yes	better	38

Students Intended: Third-party Tracking

Figure 41 and the following table 35 indicate that given a company's policies disclose the product is intended for students, does the company also disclose the qualitatively "worse" practice that they use Third-party Tracking technologies for advertising purposes.

In 2021, approximately 43% (46/107) of products intended for students also disclosed they engage in the "worse" practice of third-party tracking.

The data indicates 55% (111/200) of products disclosed that they engage in the "worse" practice using third-party tracking technologies such as cookies, unique identifiers, or fingerprinting techniques for advertising purposes whether or not students are intended users. Among the 107 products that disclose they are intended for students, approximately 41% (44/107) also disclose that they also engage in third-party tracking for advertising purposes. Additionally, among the 89 products that were "unclear" if students are intended, approximately 73% (65/89) disclose they engage in "worse" practices of third-party tracking. Products that engage in third-party tracking whether or not students are the intended audience still put students' data privacy at risk and can negatively impact learning outcomes.

Figure 41: Students Intended compared to Third-Party Tracking

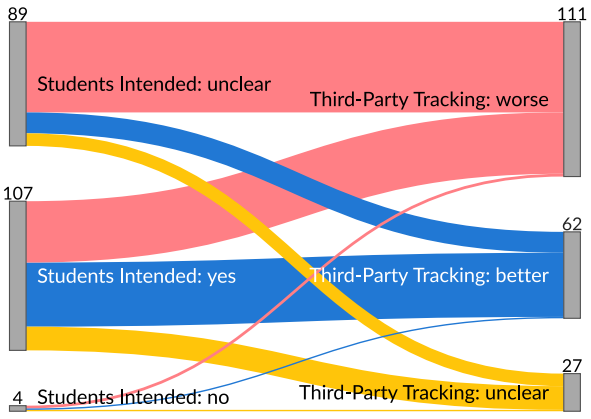


Table 35: Students Intended vs. Third-Party Tracking 2021

Students Intended	Third-Party Tracking	count
no	worse	2
no	unclear	1
no	better	1
unclear	worse	65
unclear	unclear	9
unclear	better	15
yes	worse	44
yes	unclear	17
yes	better	46

Students Intended: Track Users

Figure 42 and the following table 36 indicate that given a company's policies disclose the product is intended for students, does the company also disclose the qualitatively "worse" practice that they Track Users on other applications and services across the internet for advertising purposes.

In 2021, approximately 35% (38/107) of the products intended for students also disclosed that they engage in the "worse" practice of tracking users across the internet for advertising purposes, which is a prohibited practice if the user is a student.

The data indicates 48% (96/200) of products disclose they engage in the "worse" practice of tracking users across the internet whether or not students are intended. Among the 107 products intended for student use, approximately 36% (38/107) also disclose they engage in tracking users. These findings are surprising given that tracking students on other applications and services across the internet is a prohibited practice under federal and state student data privacy laws. Among the remaining 89 products that were "unclear" whether or not students were intended, approximately 64% (57/89) clearly disclosed they engaged in "worse" practices of tracking users. An "unclear" response on whether students are intended users of the product does not necessarily mean the product is not used in schools. Therefore, products that engage in tracking users across the internet whether or not students are the intended audience still put students' data privacy at risk and can negatively impact learning outcomes.

Figure 42: Students Intended compared to Track Users

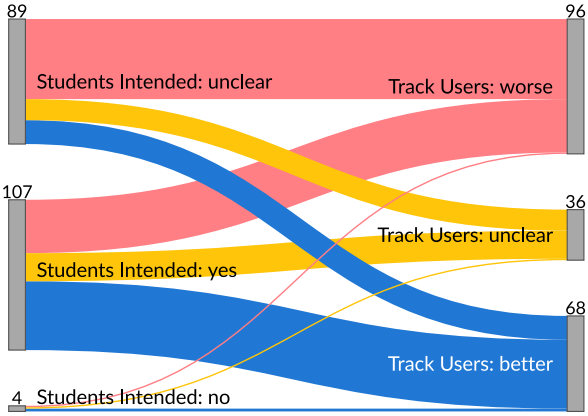


Table 36: Students Intended vs, Track Users 2021

Students Intended	Track Users	count
no	worse	1
no	unclear	1
no	better	2
unclear	worse	57
unclear	unclear	15
unclear	better	17
yes	worse	38
yes	unclear	20
yes	better	49

Students Intended: Data Profile

Figure 43 and table 37 indicate that given a company's policies disclose the product is intended for students, does the company also disclose the qualitatively "worse" practice that they amass a Data Profile about a user for advertising purposes.

The data indicates overall 40% (79/200) of products disclose they engage in the "worse" practice of creating an advertising profile of a user whether or not students are intended. Among the 107 products intended for students, there is a three-way split with approximately 26% (28/107) that remain "unclear" about profiling, 47% (50/107) disclose "better" practices that they do not create a profile, but 27% (29/107) disclose the "worse" practice that they create an advertising profile of users. These findings are surprising given that amassing an advertising profile of students for advertising purposes is a prohibited practice under federal and state student data privacy laws.

In 2021, approximately 27% (29/107) of products intended for students also disclosed they engage in the "worse" and prohibited practice of amassing a profile of a student for advertising purposes.

Products that disclose students are the intended audience but also disclose they create data profiles of users may be limiting data profile creation to only adult users, such as teachers and other school officials. However, products often allow students to create accounts with a product that may not have been designed for educational purposes and without any additional student data privacy agreement in place with the school or district, which could inadvertently expose students to "worse" data profile creation practices unless the company has actual knowledge that the user is a student and avoids amassing a data profile for the student in question. Therefore, products that create advertising data profiles of users whether or not students are the intended audience still put students' data privacy at risk and can negatively impact learning outcomes.

Figure 43: Students Intended compared to Data Profile

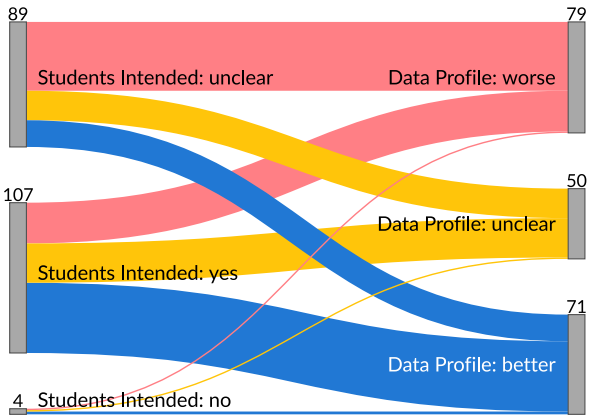


Table 37: Students Intended vs. Data Profile 2021

Students Intended	Data Profile	count
no	worse	1
no	unclear	1
no	better	2
unclear	worse	49
unclear	unclear	21
unclear	better	19
yes	worse	29
yes	unclear	28
yes	better	50

Evaluation Concerns

The evaluation concerns summarize the policies of an application or service into categories based on a focused subset of evaluation questions that can be used to quickly identify the strengths and weaknesses of a company's policies. Ten different concerns have been created based on feedback from consumers, parents, and educators on the most important questions they have about a product's privacy practices. Each concern is composed of 10 of the most important evaluation questions that are related to the respective category. The 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 strengths and weaknesses with respect to the specific concern and other products.

The privacy evaluation concerns are identified 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 38 and Table 39 summarize our findings for 2020 and 2021 of the minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 38: 2020 concern score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
Data Collection	0	40	50	50	60	80
Data Sharing	0	69	80	74	85	95
Data Security	0	35	55	56	75	95
Data Rights	0	55	75	70	85	95
Individual Control	0	35	50	50	65	95
Data Sold	0	30	40	41	55	95
Data Safety	0	25	45	41	60	90
Ads & Tracking	0	40	60	54	65	95
Parental Consent	0	45	65	58	75	95
School Purpose	0	0	32	34	60	85

The 2020 concern category score descriptive statistics are shown for reference to concern scores in 2021. Even where minimum, maximum, or median scores for a particular concern indicate no significant changes in the short term, there can still be significant changes within the ten questions that comprise each concern. Individual question changes may not be reflected in the median score. Therefore, it is important to examine all the questions within each concern category to determine what changes, if any, have actually occurred since 2020 and whether they have contributed to changes in the concern's minimum, maximum, or median scores or not.

Table 39: 2021 concern score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
Data Collection	15	45	50	51	60	80
Data Sharing	10	70	80	75	85	95
Data Security	0	35	55	54	75	100
Data Rights	0	60	75	72	85	95
Individual Control	5	35	45	50	60	95
Data Sold	0	30	40	41	55	95
Data Safety	0	29	45	42	60	90
Ads & Tracking	0	45	60	54	65	95
Parental Consent	0	40	60	56	75	95
School Purpose	0	0	30	33	60	90

The 2021 concern category scores indicate a wide range of minimum to maximum scores, with many scores indicating no significant changes since 2020. The following 10 concern categories take a closer look at short- and long-term changes.

Data Collection

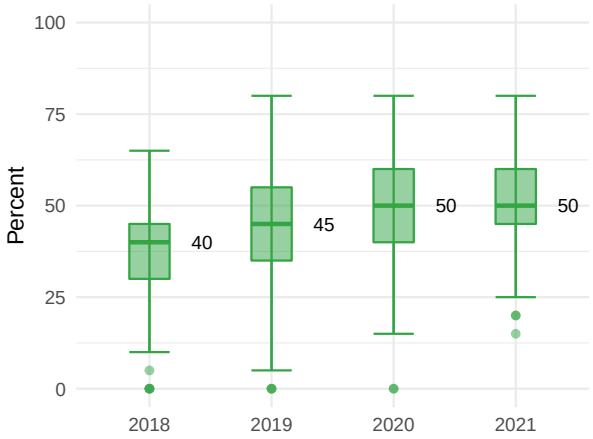
The Data Collection concern category indicates whether the product has responsible data collection practices that limit the type and amount of personal information collected about users to only what's necessary to provide the application or service. Figure 44 illustrates the Data Collection product score spread among all products evaluated. Table 40 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 40: Year-over-year results Data Collection score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	30	40	38	45	65
2019	0	35	45	45	55	80
2020	0	40	50	50	60	80
2021	15	45	50	51	60	80

From the analysis of the 10 questions in the Data Collection concern, we determined a median in 2021 of approximately 50%. This median is lower than expected, given that these products 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. The median score appears to be stable at 50%, but as discussed below, the minimum and Q1 score improved considerably (lower whisker, and IQR). This means that while the median score was static, the industry standard on the lower end has improved in 2021.

Figure 44: Comparison of Data Collection scores year-over-year results



Since 2020, the Data Collection category median scores are stable, and have a stable maximum score but with an increase in the minimum score. Compared to 2018, applications and services evaluated in 2021 for the concern of Data Collection indicate a year-over-year 25% increase in median scores, which translates to more transparent and qualitatively "better" practices with respect to the collection of personal information.

There is still room for improvement. Industry norms have improved as the result of more specific laws and regulations as well as consumer frustration with inadequate privacy protections. As a result, some applications and services are now considered extreme outliers providing a level of detail below industry norms and their policies should be updated to address these shortcomings. The increase in the minimum scores indicate a potential trend for "better" transparency related to the Data Collection concern, and in 2022 we hope to see more policies updating their terms to address shifting legislative requirements and user concerns about what types of personal information are collected by the product.

Table 41: Data Collection question response percentage point change from 2020 to 2021

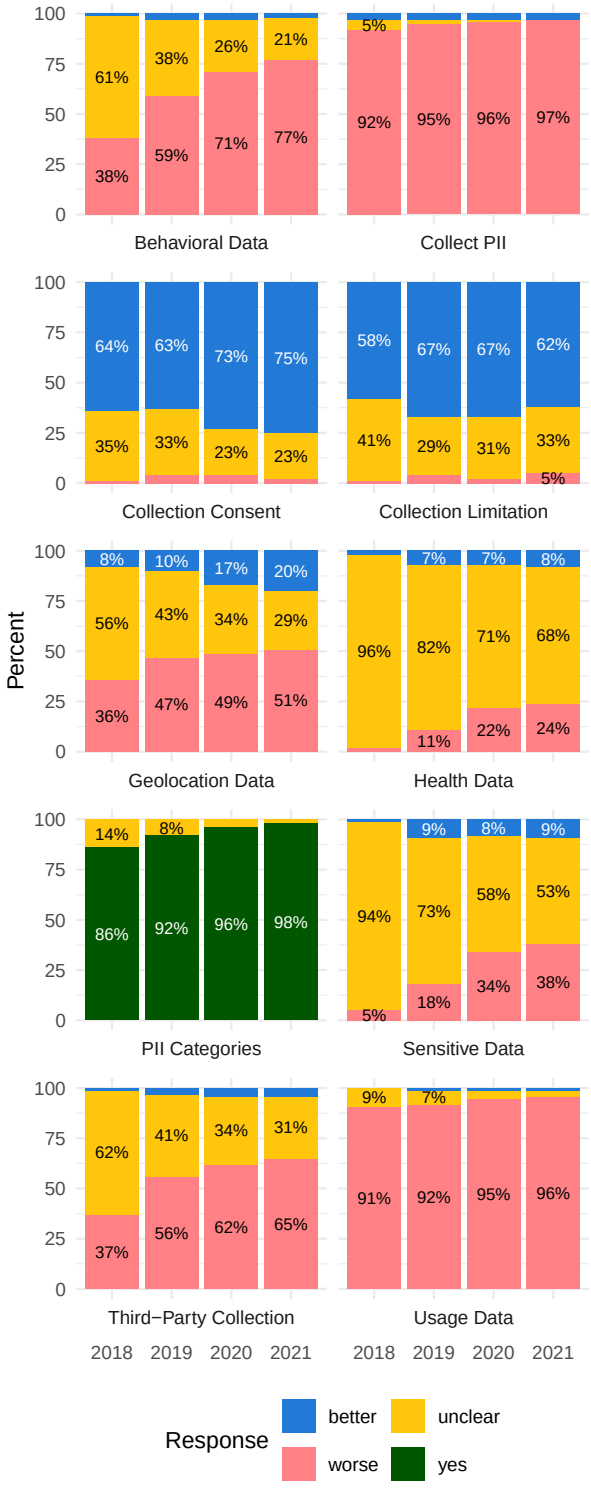
Question	"better"	"worse"	"unclear"	Yes
Behavioral Data	-1	6	-4	NA
Collect PII	0	2	NA	NA
Collection Consent	2	-2	-1	NA
Collection Limitation	-4	4	1	NA
Geolocation Data	3	3	-6	NA
Health Data	1	2	-2	NA
PII Categories	NA	NA	-2	2
Sensitive Data	0	4	-4	NA
Third-Party Collection	0	3	-2	NA
Usage Data	-1	1	-1	NA

The Data Collection concern category median score is stable at 50%, but figure 45 indicates generally decreasing "unclear" policies as well as increases to "worse" responses within the concern category. In the aggregate this did not change the median score, but the increased transparency did increase the minimum score. In addition, many of the questions in this concern category indicate increases in "worse" practices in 2021, which mean products either increased their transparency for existing practices or increased the amount of data they collect from users as well as the different types of data they collect. For example, the Behavioral Data and Sensitive Data evaluation questions indicate a reduction in non-transparent or "unclear" policies, resulting in an increase in "worse" practices that involve the increased collection of behavioral and sensitive data. In addition, the Collection Limitation indicates a negative shift from "better" to "worse" practices. The risk of asking the question, of course, is getting the answer, and we realize as regulations require companies to be more transparent that they will, in some cases, disclose "worse" practices. Overall, this increased transparency, even without the hoped-for transformation into "better" practices, is an improvement over keeping consumers in the dark.

Data Sharing

The Data Sharing concern category indicates whether the product has data sharing best practices that protect a person's personal information from being shared with third-party companies and

Figure 45: Data Collection question response change year-over-year results.



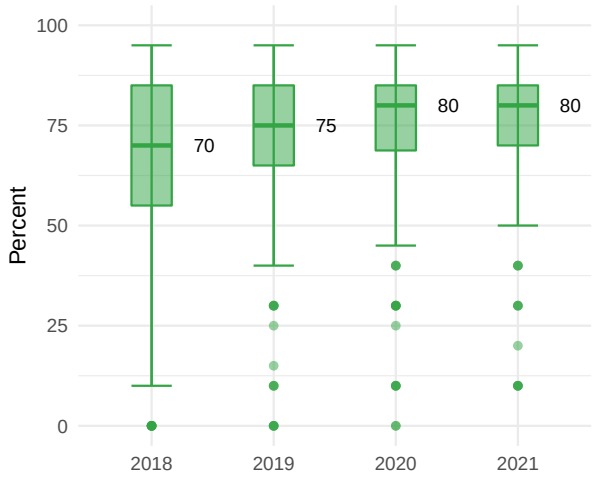
advertisers. Figure 46 illustrates the Data Sharing median scores among all products evaluated. Table 42 compares and summarizes the Data Sharing concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 42: Year-over-year results Data Sharing score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	55	70	64	85	95
2019	0	65	75	70	85	95
2020	0	69	80	74	85	95
2021	10	70	80	75	85	95

From the analysis of the 10 questions in the Data Sharing concern, we determined a median in 2021 of approximately 80%, which is the highest score across all concern categories. This higher-than-average median is expected, given that these products are intended for children and students and that a majority of companies disclose qualitatively "better" practices about sharing data, including whether they share data with third parties and the purposes for which they share data. The median score, as well as all other descriptive statistics, appear to be stable, which indicates that Data Sharing-related industry practices are not getting "better" or "worse" but that companies are still not disclosing their practices on the remaining issues in this category.

Figure 46: Comparison of Data Sharing scores year-over-year results



Since 2020 the Data Sharing category median scores are stable, and have a stable maximum and minimum score. Compared to 2018, applications and services evaluated in 2021 for the concern of Data Sharing indicate a 14% increase in median scores that translate to more transparent and qualitatively "better" practices with respect to sharing personal information with third parties to provide the product. Additionally, industry norms have improved since 2018, but some applications and services are still providing a level of detail below industry norms and their policies should be updated to address these shortcomings.

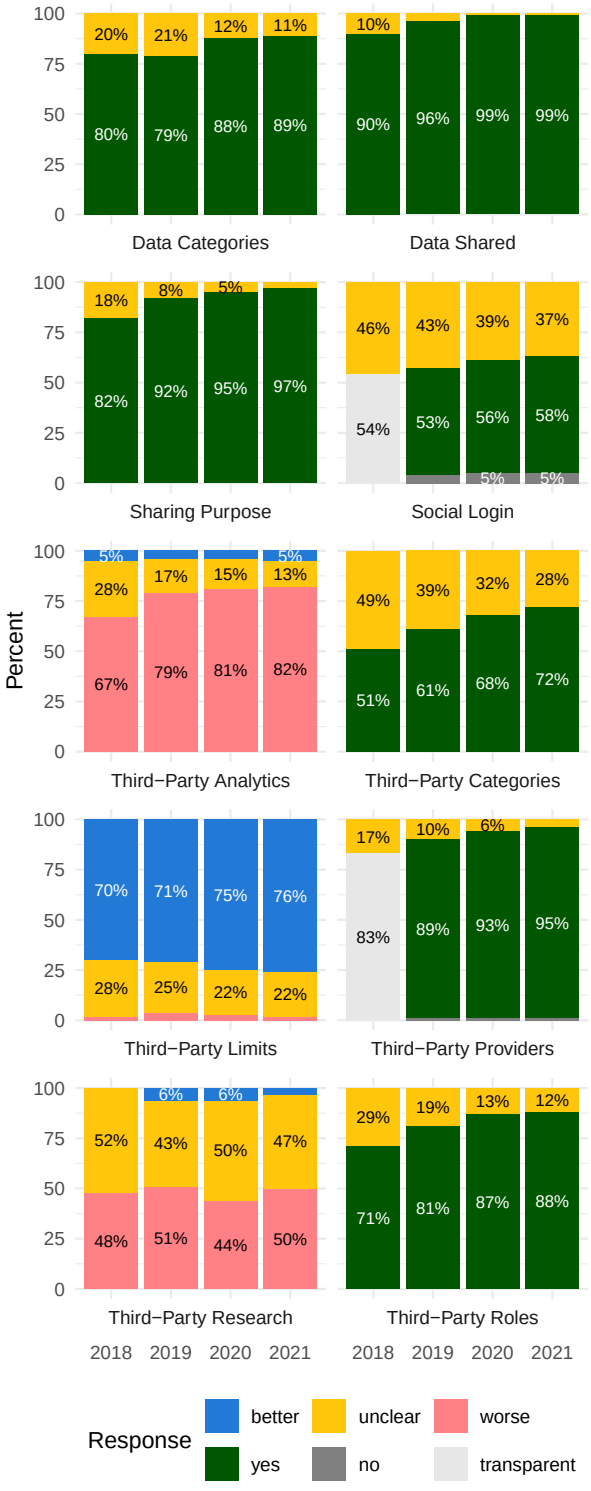
Table 43: Data Sharing question response percentage point change from 2020 to 2021

Question	"better"	"worse"	"unclear"	No	Yes
Data Categories	NA	NA	-1	NA	1
Data Shared	NA	NA	0	NA	0
Sharing Purpose	NA	NA	-1	NA	1
Social Login	NA	NA	-2	0	1
Third-Party Analytics	0	0	-2	NA	NA
Third-Party Categories	NA	NA	-4	NA	4
Third-Party Limits	2	-1	0	NA	NA
Third-Party Providers	NA	NA	-2	0	3
Third-Party Research	-3	6	-3	NA	NA
Third-Party Roles	NA	NA	-2	NA	2

Although the Data Sharing concern category median score is stable at 80%, figure 47 indicates some positive and negative transparency changes within the concern category that did not impact the median score. This concern category consists of a higher percentage of transparency only questions that do not have a "better" or "worse" qualitative component, as indicated by "NA" in the "better," "worse," and "unclear" columns in Table 43. This higher proportion of questions that only indicate transparency could help explain the higher-than-average median score compared to the other concern categories, as transparency is easier to achieve as compared to questions that have qualitative components and may require longer explanations, or may include "worse" disclosures resulting in fewer points earned.

In addition, many of the questions in this concern category indicate positive shifts from

Figure 47: Data Sharing question response change year-over-year results.



non-transparency or "unclear" to disclosing the company's practices about the issue raised in the question. For example, the Data Categories, Sharing Purpose, Third-party Categories, and Third-party Roles evaluation questions all indicate a positive trend from non-transparent or "unclear" policies to disclosing the details of the types of data shared with third parties, the purpose for sharing that data, and the categories of third parties involved. The element of data sharing is significant to users' concerns about giving their personal information to an intended company, the first party, and not to myriad other companies. Other companies are designated as third parties in the system, but the economic ecosystem of data sharing and sales means that there are not just third parties, but fourth, fifth and so on as data is sold, shared, combined, and used in different contexts and for a variety of financial purposes.

Data Security

The Data Security concern category indicates whether the product has data security best practices that protect the integrity and confidentiality of a person's data. Figure 48 illustrates the Data Security median scores among all products evaluated. Table 44 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).

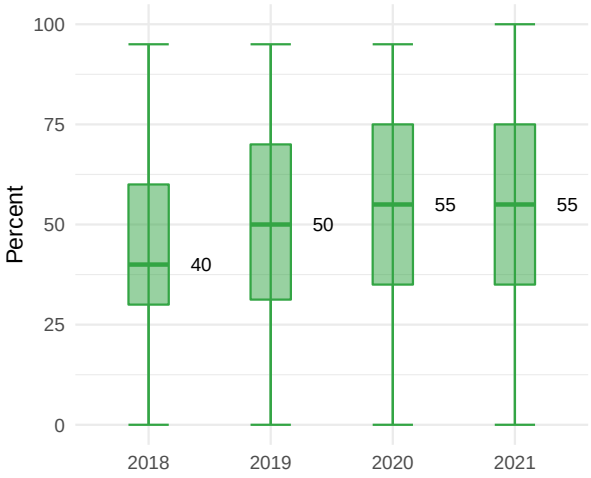
Table 44: Year-over-year results Data Security score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	30	40	44	60	95
2019	0	31	50	53	70	95
2020	0	35	55	56	75	95
2021	0	35	55	54	75	100

From the analysis of the 10 questions in the Data Security concern, we determined a median in 2021 of approximately 55%. This median is lower than expected, given that these products are intended for children and students and that a majority of companies disclose qualitatively "better" practices that they use reasonable security practices to protect users' personal information collected by the

product. The median score appears to be stable at 55% which indicates that Data Security-related industry practices are not getting "better" or "worse," but that companies are still not disclosing their practices on the remaining issues in this category.

Figure 48: Comparison of Data Security scores year-over-year results



Since 2020 the Data Security category median scores are stable, and have a stable minimum score but an increase in the maximum score. Compared to 2018, applications and services evaluated in 2021 for the concern of Data Security indicate an approximate 38% increase in median scores that translate to more transparent and qualitatively "better" practices with respect to protecting users' personal information from unauthorized disclosure. Additionally, security practices need to be constantly updated and processes improved as a result of lessons learned from data breaches and ransomware attacks since 2018, but some applications and services are still providing a level of security detail below industry standards and their policies should be updated to address these shortcomings. Hopefully in 2022 we will see more policies updating their terms to disclose "better" practices in this category regarding what tools and processes companies use to actually protect users' personal information.

Table 45: Data Security question response percentage point change from 2020 to 2021

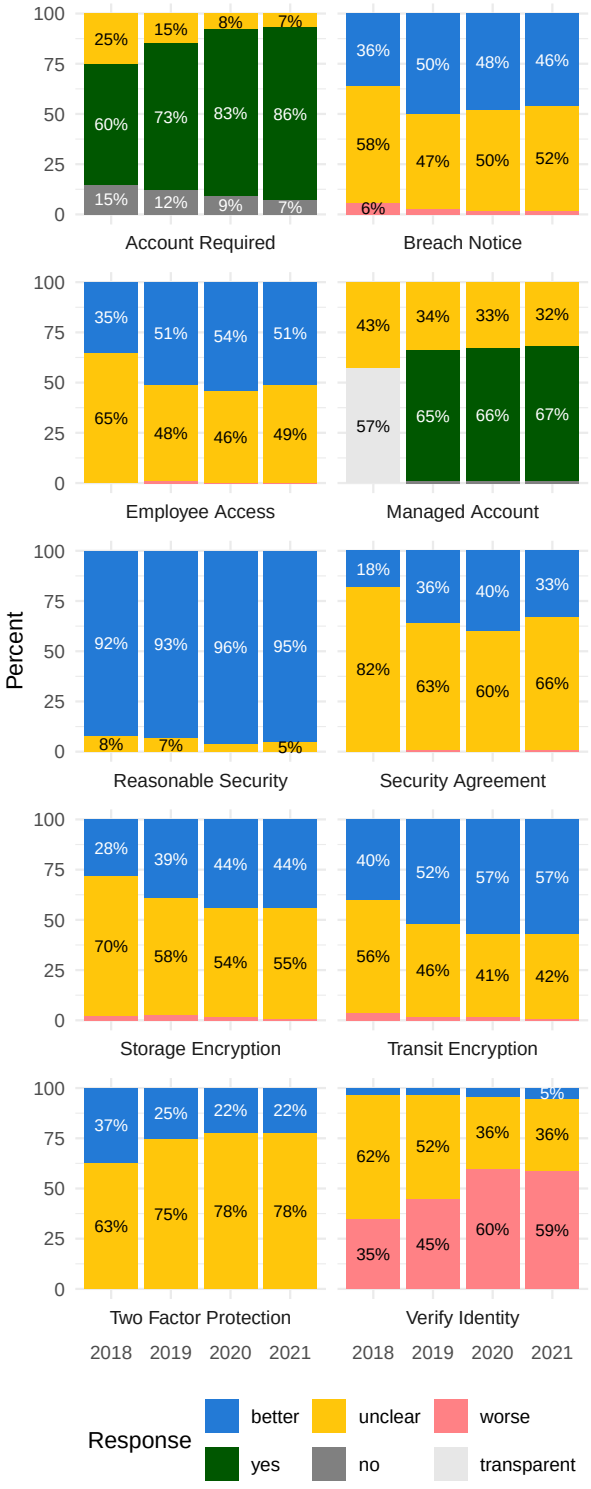
Question	"better"	"worse"	"unclear"	No	Yes
Account Required	NA	NA	-1	-2	4
Breach Notice	-2	0	2	NA	NA
Employee Access	-3	0	2	NA	NA
Managed Account	NA	NA	-2	0	0
Reasonable Security	-1	0	0	NA	NA
Security Agreement	-8	1	6	NA	NA
Storage Encryption	0	0	1	NA	NA
Transit Encryption	-1	0	1	NA	NA
Two Factor Protection	0	0	0	NA	NA
Verify Identity	0	0	0	NA	NA

Although the Data Security concern category median score is stable at 55%, table 45 indicates some small transparency gains and losses, but also shows that negative qualitative changes within the concern category did not impact the median score. For example, the Account Required and Manage Account evaluation questions indicate a positive shift from non-transparent or "unclear" policies to disclosing whether users are able to create accounts and manage accounts with parental controls through the product to protect users' personal information. However, there was also a decrease in "better" practices with a shift to non-transparency or "unclear" for the Breach Notice, Employee Access, and Security Agreement evaluation questions. Overall, the individual questions in this concern indicate a widespread lack of transparency, with four questions indicating over half of products lack any details about those respective practices.

While "industry-standard security" is a term often referenced in policies, it is nebulous, and our data shows that there is no clear definition of what "industry best practices" means with products including the full range 0-to-100.

There was a significant shift in 2021 on the Security Agreement evaluation question from "better" to non-transparent or "unclear" practices regarding whether a company has a security agreement with

Figure 49: Data Security question response change year-over-year results.



third-party service providers that help provide the product. Security agreements with third-party service providers are considered a qualitatively "better" practice, because they can often mitigate complex compliance burdens on companies to implement expensive security procedures, which "better" protects the data of children and students. In some cases, "unclear" policies may be the result of companies otherwise meeting their compliance obligations by composing internal security policies to enforce their physical and network security standards. In other cases, companies may work with dozens of third-party service providers and subcontractors under non-disclosure agreements of their security practices. Companies may believe that consumers do not need to know this relatively technical and proprietary information, and they may believe disclosing these policies would be a competitive disadvantage. Still, we believe there is value in transparency on security as well as privacy, and that these protocols, perhaps summarized for non-technical users, deserve space in the public-facing policies.

Data Rights

The Data Rights concern category indicates whether the product provides the ability for users to exercise their data rights that include the ability to review, access, modify, delete, and export their personal information and content. Figure 50 illustrates the Data Rights median scores among all products evaluated. Table 46 compares and summarizes the Data Rights concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

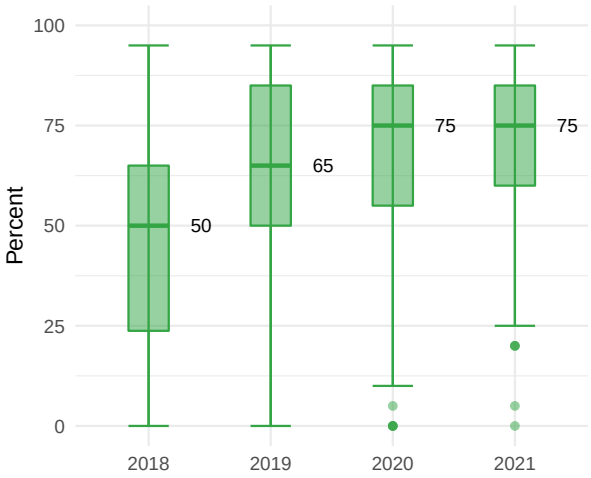
Table 46: Year-over-year results Data Rights score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	24	50	44	65	95
2019	0	50	65	63	85	95
2020	0	55	75	70	85	95
2021	0	60	75	72	85	95

From the analysis of the 10 questions in the Data Rights concern, we determined a median score in 2021 of approximately 75%, which is

the second-highest concern category median score. This higher median score is expected, given that these products are intended for children and students and that a majority of companies disclose qualitatively "better" practices that users can access, modify, delete, and export their information from the product at any time. The median score and other descriptive statistics appear to be stable, which indicates that Data Rights-related industry practices are not getting "better" or "worse," but companies are still not disclosing their practices on the remaining issues in this category.

Figure 50: Comparison of Data Rights scores year-over-year results



Since 2020 the Data Rights category median scores are stable and have a stable maximum score, but since 2018 there has been a significant increase in the Q1 score. This indicates that industry norms in the lower or first quartile have significantly improved since 2018. Compared to 2018, applications and services evaluated in 2021 for the concern of Data Rights indicate a 50% increase in median scores that translate to more transparent and qualitatively "better" practices with respect to the ability of users to exercise their privacy rights with the product or company.

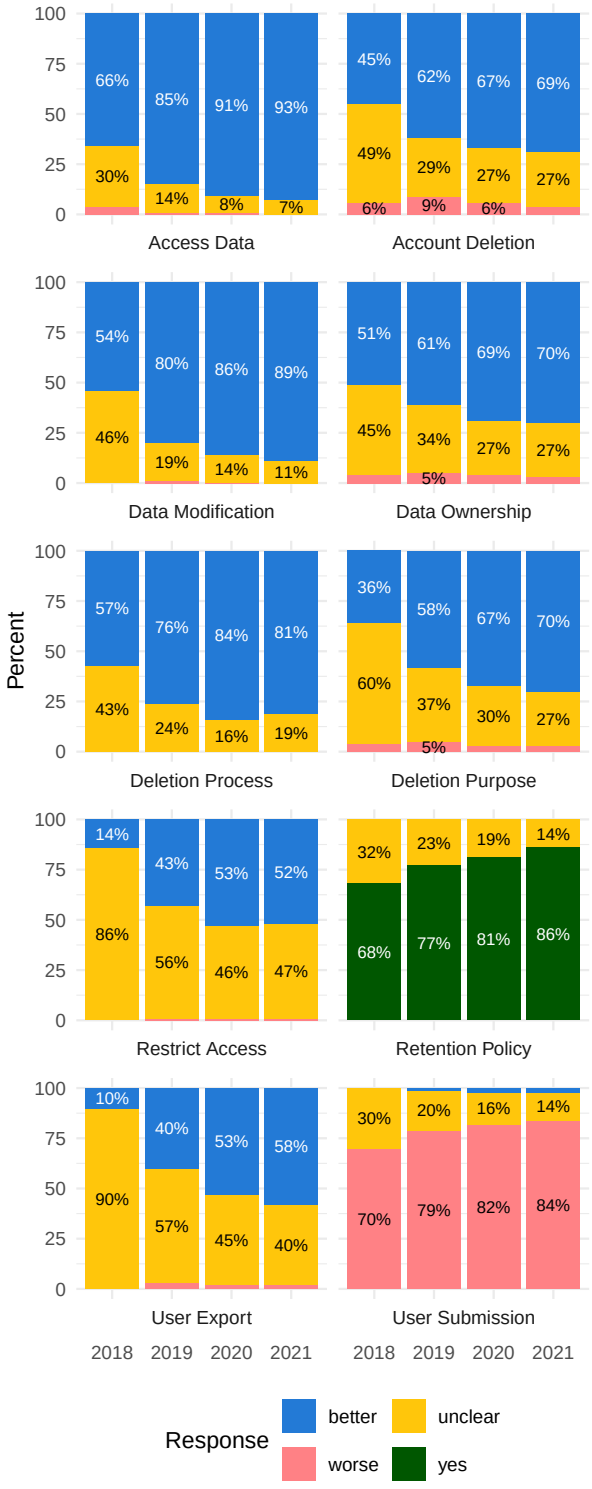
Additionally, since GDPR and follow-on state laws have improved this standard since 2019, some applications and services are now providing a level of detail below industry norms and their policies should be updated to address these shortcomings. Hopefully the increase in the Q1 scores indicate a trend for "better" transparency related to the Data Rights concern, and in 2022 we will see more outliers updating their terms to disclose privacy rights they may already provide to users but do not disclose in their policies.

Table 47: Data Rights question response percentage point change from 2020 to 2021

Question	"better"	"worse"	"unclear"	Yes
Access Data	2	-1	-2	NA
Account Deletion	2	-2	-1	NA
Data Modification	2	0	-3	NA
Data Ownership	1	0	0	NA
Deletion Process	-4	NA	3	NA
Deletion Purpose	3	-1	-3	NA
Restrict Access	0	0	2	NA
Retention Policy	NA	NA	-6	6
User Export	5	0	-4	NA
User Submission	0	2	-2	NA

Although the Data Rights concern category median score is stable at 75%, table 46 indicates some significant positive transparency changes, with nearly all of those gains being positive qualitative changes that in the aggregate did not change the median score. For example, the Access Data, Data Modification, Deletion Purpose, User Export and Retention Policy evaluation questions indicate a positive trend from non-transparent or "unclear" policies to transparent or qualitatively "better" disclosures that users are able to access, modify, delete, and export their data from the product with notice of the product's data retention time period.

Figure 51: Data Rights question response change year-over-year results.



Individual Control

The Individual Control concern category indicates whether the product allows users to exercise control over what personal data companies collect from them and to prevent its use for incompatible purposes. Figure 52 illustrates the Individual Control median scores among all products evaluated. Table 48 compares and summarizes the Individual Control concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 48: Year-over-year results Individual Control score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	30	40	42	55	85
2019	0	30	45	46	60	95
2020	0	35	50	50	65	95
2021	5	35	45	50	60	95

From the analysis of the 10 questions in the Individual Control concern, we determined a median in 2021 of approximately 45%. This low median score is unexpected, given that these products are intended for children and students and that a majority of companies disclose qualitatively "better" practices that users' data is not used for incompatible purposes or combined with other data and shared with third parties that could lead to unintended purposes. While the median score did change, the other descriptive statistics appear to be stable which indicates that Individual Control related industry practices are not getting "better" or "worse" and companies still have significant room for improvement in disclosing practices on the issues in this category.

Compared to 2018, applications and services evaluated in 2021 for the concern of Individual Control indicate a 13% increase in the median score with slight increases in the minimum and maximum scores over the past four years. Due to the relative stability of the descriptive statistics, many of the issues in this concern have not been addressed adequately by companies, but a closer examination of the questions that make up this concern category indicate several shifts both positive and negative.

Figure 52: Comparison of Individual Control scores year-over-year results

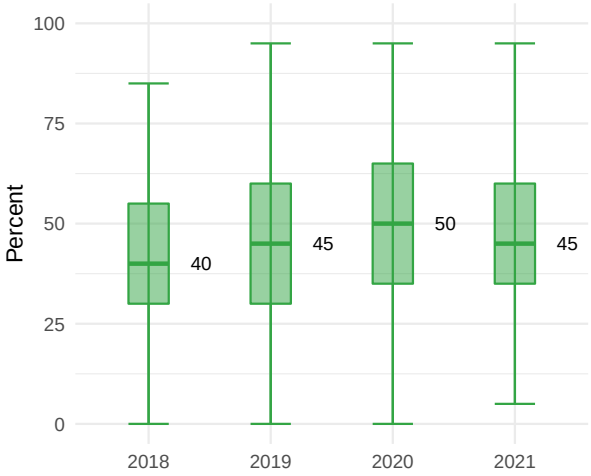


Table 49: Individual Control question response percentage point change from 2020 to 2021

Question	"better"	"worse"	"unclear"	Yes
Combination Type	-4	-1	5	NA
Complaint Notice	4	0	-3	NA
Context Consent	-4	0	4	NA
Context Notice	-3	-1	4	NA
Data Purpose	NA	NA	0	0
Disclosure Notice	2	0	-2	NA
Disclosure Request	-1	1	1	NA
Purpose Limitation	-7	0	6	NA
User Control	6	NA	-6	NA
Vendor Combination	2	2	-4	NA

Although the Individual Control concern category median score is stable at 45%, table 49 indicates some significant transparency changes as well as both positive and negative qualitative changes within the concern category that in the aggregate did not change the median score. For example, the Complaint Notice, Disclosure-Notice, User Control, and Vendor Combination evaluation questions indicate a positive trend from non-transparent or "unclear" policies to "better" disclosures that users have privacy controls and users will receive notice if their account is blocked or if their data is shared with third parties. Specifically, the complaint notice evaluation question likely increased transparency in response

Figure 53: Individual Control question response change year-over-year results.

to compliance requirements in the GDPR and CCPA that require a company to have an independent grievance or remedy mechanism for users to file a complaint if the company does not respect a user's privacy choices.

However, this increase in transparency is offset by a decrease in "better" practices and an increase in companies no longer disclosing issues they once disclosed in their policies. For example, the Combination Type, Context Consent, Context Notice, and Purpose Limitation evaluation questions all shifted from "better" disclosures to "unclear," which indicates a shift in the industry not to disclose the purpose for which data is collected and used by the product which could conflict with incompatible purposes.

This privacy-regressive shift is likely a compliance-motivated decision to remove specific disclosures in a company's policies that explain the purpose for which a user's data is collected or combined. This change could be interpreted to mean companies are moving away from transparency on particular issues in order to allow them the legal flexibility to use data in unintended ways without notice or consent from users, because the additional purpose could be incompatible with the previously specified purposes in their policies that were removed in 2021. Companies should disclose the purpose for which personal data is collected by the product because there is an increased risk to users if the data is used for unintended purposes not related to providing the services and an increased risk to the company of financial loss through statutory fines or reputational damages.

Data Sold

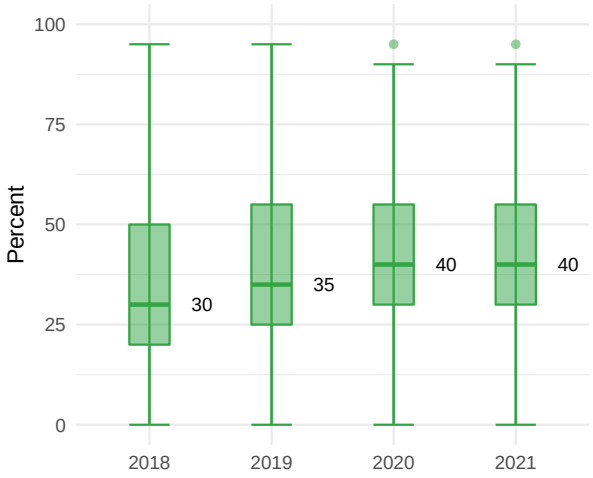
The Data Sold concern category indicates whether the product shares, rents, or sells a person's personal information to third parties for monetary value or other financial gain. Figure 54 illustrates the Data Sold median scores among all products evaluated. Table 50 compares and summarizes the Data Sold concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 50: Year-over-year results Data Sold score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	20	30	35	50	95
2019	0	25	35	40	55	95
2020	0	30	40	41	55	95
2021	0	30	40	41	55	95

From the analysis of the 10 questions in the Data Sold concern, we determined a median in 2021 of approximately 40%, which is the lowest score among all the concern categories. This low median score is unexpected, given that these products are intended for children and students and that companies should disclose qualitatively "better" practices that children's data is not sold to third parties. The median score, and other descriptive statistics, also appear to be stable, which indicates that Data Sold-related industry practices are not getting "better" or "worse" but that companies are still not disclosing "better" practices on selling data even with recent privacy legislation primarily focused on this issue.

Figure 54: Comparison of Data Sold scores year-over-year results



Compared to 2018, applications and services evaluated in 2021 for the concern of Data Sold indicate a 33% increase in median scores that translate to more transparent and qualitatively "better" practices with respect to monetizing users' data through various data collection methods, including selling data to third parties.

Although industry norms have improved since 2018, the majority of applications and services are still providing a low level of detail in their policies about their data monetization practices that do not align with their privacy compliance obligations. It appears that because the median score is so low and has not changed over the short term, many of the issues in this concern have not been addressed adequately by companies. However, a closer examination of the questions that make up this concern category indicate several shifts, both positive and negative.

Table 51: Data Sold question response percentage point change from 2020 to 2021

Question	"better"	"worse"	"unclear"	No	Yes
Combination Limits	0	0	0	NA	NA
Contractual Limits	-2	0	2	NA	NA
Data De-identified	NA	NA	-1	-2	2
De-identified Process	-3	NA	3	NA	NA
Delete Transfer	-1	0	1	NA	NA
Opt Out Consent	3	0	-2	NA	NA
Sell Data	1	5	-6	NA	NA
Third-Party Research	-3	6	-3	NA	NA
Transfer Data	0	-2	2	NA	NA
Transfer Notice	0	-2	2	NA	NA

Although the Data Sold concern category median score is stable at 40%, table 51 indicates some positive transparency changes and both positive and negative qualitative changes within the concern category that in the aggregate did not significantly impact aggregate industry scores. For example, the Sell Data, Transfer Data, and Transfer Notice evaluation questions indicate a positive trend from non-transparent or "unclear" policies to qualitatively "worse" practices that allow companies to monetize users' data by selling it to third parties, or in the event of an acquisition or merger a user's data is a valuable asset that can be transferred to the successor company without notice to users.

There were "better" qualitative changes for the Opt-out Consent evaluation question, but qualitatively "worse" changes for the Data De-identified and De-identified Process evaluation questions, which indicates that companies are also monetizing users' de-identified or anonymized data with third parties

Figure 55: Data Sold question response change year-over-year results.

and also providing the ability for users to opt out of some, but not all, of these "worse" practices. Lastly, there was an increase in "worse" practices with the Third-party Research evaluation question that indicates a shift away from "better" and "unclear" practices because more companies are disclosing that they now share users' data with third parties for research purposes, which is another user data monetization business model for de-identified or anonymized data. Disclosing collected information in an anonymous or de-identified format is a complicated issue, and even data that has gone through this process can often be recombined with other data easily to allow re-identification by third parties, as indicated in our Combination Limits evaluation question. As such, the sharing of any information, even information about a user that has been de-identified or anonymized, is a privacy risk.

Data Safety

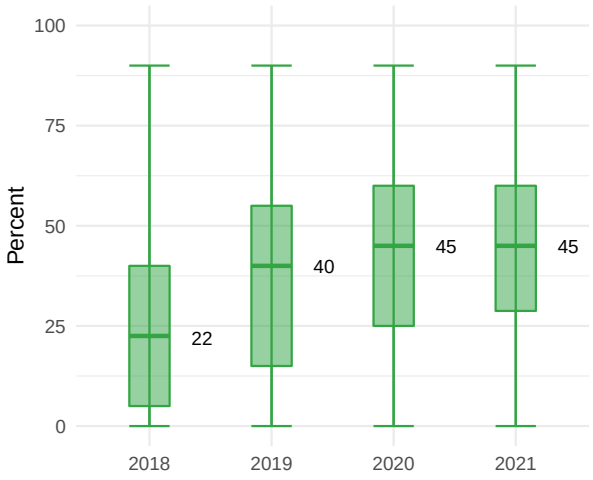
The Data Safety concern category indicates whether the product limits the visibility of a person's information and their interactions with others to protect their physical and emotional well-being. Figure 56 illustrates the Data Safety median scores among all products evaluated. Table 52 compares and summarizes the Data Safety concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 52: Year-over-year results Data Safety score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	5	22	26	40	90
2019	0	15	40	36	55	90
2020	0	25	45	41	60	90
2021	0	29	45	42	60	90

From the analysis of the 10 questions in the Data Safety concern, we determined a median in 2021 of approximately 45%. This low median score is unexpected, given that these products are intended for children and students and that companies should disclose qualitatively "better" practices that increase the safety of children using their products. The median score also appears to be stable at 45%, which indicates that Data Safety-related industry practices are not getting "better" or "worse" but that companies are still not disclosing practices about protecting the safety of children when interacting with other trusted and untrusted users, or monitoring harmful content or abuse.

Figure 56: Comparison of Data Safety scores year-over-year results



Since 2020, the Data Safety category median scores are stable and have a stable minimum and maximum score. Compared to 2018, applications and services evaluated in 2021 for the concern of Data Security indicate a 105% increase in median scores, which translates to more transparent and qualitatively "better" practices with respect to protecting users from unsafe interactions. Additionally, industry norms have improved significantly since 2018, but many applications and services are still providing little or no detail and their policies should be updated to address these shortcomings. Hopefully in 2022 we will see more policies updating their terms to disclose "better" practices in this category regarding what tools and procedures companies use to protect users, particularly child users, from inappropriate content or interactions.

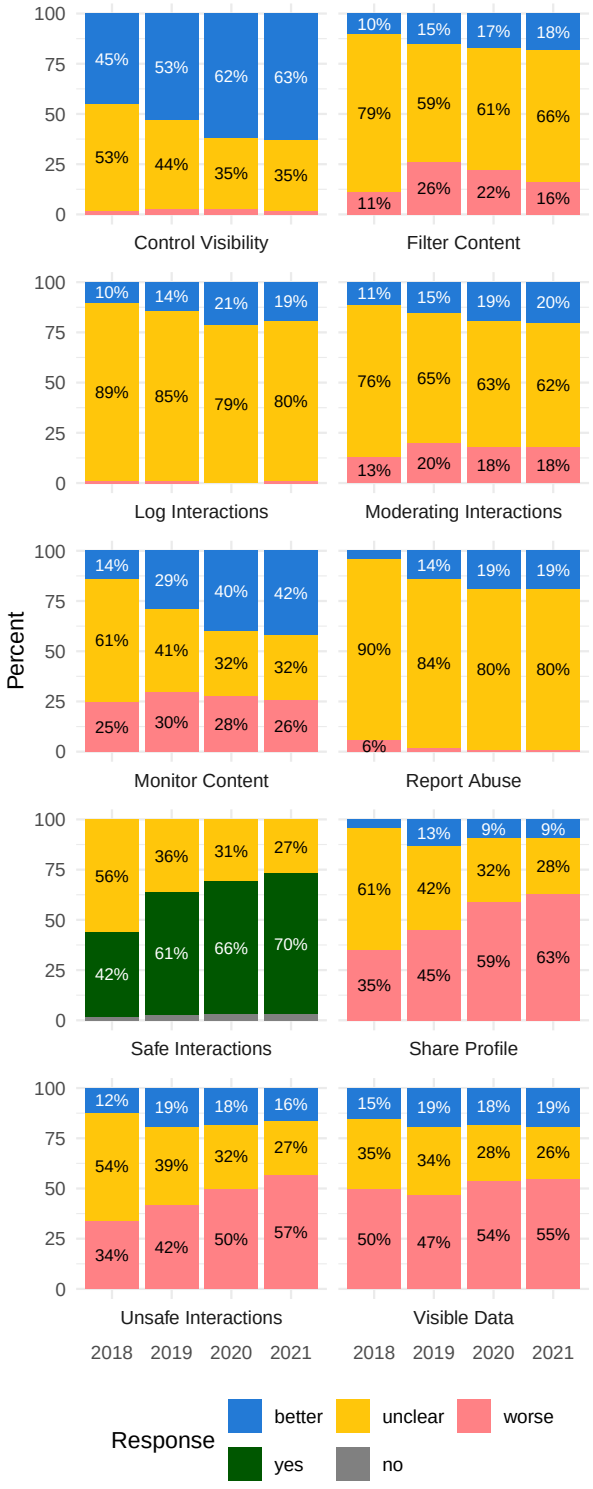
Table 53: Data Safety question response percentage point change from 2020 to 2021

Question	"better"	"worse"	"unclear"	No	Yes
Control Visibility	0	-1	0	NA	NA
Filter Content	1	-6	5	NA	NA
Log Interactions	-2	NA	1	NA	NA
Moderating Interactions	1	0	-1	NA	NA
Monitor Content	2	-2	0	NA	NA
Report Abuse	0	1	0	NA	NA
Safe Interactions	NA	NA	-5	0	4
Share Profile	-1	4	-4	NA	NA
Unsafe Interactions	-2	7	-4	NA	NA
Visible Data	1	2	-2	NA	NA

Although the Data Safety concern category median score is stable at 45%, table 53 indicates some positive transparency changes and both positive and negative qualitative changes within the concern category that did not impact the median score. For example, the Share Profile, Unsafe Interactions, and Visible Data evaluation questions indicate an increase from non-transparent or "unclear" policies to qualitatively "worse" practices that allow users to share personal information about themselves to others on the product for unsafe interactions with users they do not know in real life and make their profile publicly visible online. However, there was also a shift from "worse" practices to non-transparency or "unclear" with the Filter Content evaluation question which indicates products are not putting in place adequate protections to prevent children from disclosing personal information to other users of the product or to prevent children from making personal information publicly visible. Overall, the individual questions in this concern indicate a widespread lack of transparency, with four questions indicating over half of products lack any details about those respective practices.

In addition, there were "better" qualitative changes for the Monitor Content and Safe Interactions evaluation questions, which indicates that companies are also putting in place processes to monitor inappropriate content as products increase the numbers of both safe and unsafe interactions.

Figure 57: Data Safety question response change year-over-year results.



Ads & Tracking

The Ads & Tracking concern category indicates whether the product provides responsible advertising practices that limit the use of personal information for any third-party marketing, targeted advertising, tracking, or profile generation purposes. Figure 58 illustrates the Ads & Tracking median scores among all products evaluated. Table 54 compares and summarizes the Ads & Tracking concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

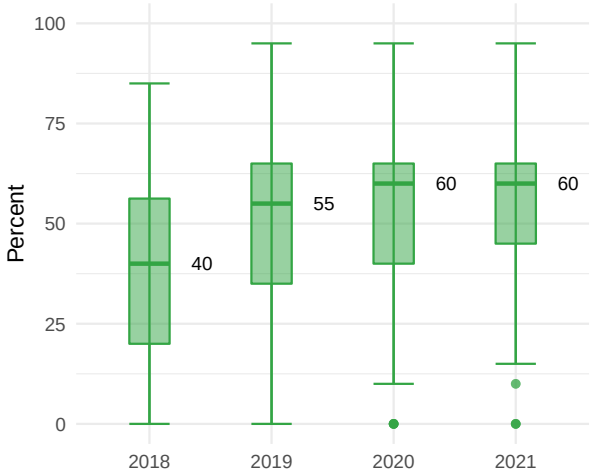
Table 54: Year-over-year results Ads & Tracking score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	20	40	38	56	85
2019	0	35	55	50	65	95
2020	0	40	60	54	65	95
2021	0	45	60	54	65	95

From the analysis of the 10 questions in the Ads & Tracking concern, we determined a median score in 2021 of approximately 60%. This low median score is unexpected, given that these products are intended for children and students and that companies should disclose qualitatively "better" practices that the product does not display targeted advertisements or track users on other applications and services across the internet. The median score and most of the other descriptive statistics also appear to be stable, but the percentage change in the questions within the category indicate that Ads & Tracking-related industry practices are increasing in transparency but disclosing "worse" practices. Companies are still not disclosing "better" practices about protecting children and students from prohibited practices such as targeted advertising and tracking on their products.

Since 2020 the Ads & Tracking category median score is stable and has a stable maximum score but an increase in the Q1 score. Compared to 2018, applications and services evaluated in 2021 for the concern of Ads & Tracking indicate a 50% increase in median scores, which translates to more transparent and qualitatively "better" practices of not displaying targeted advertisements to users or tracking users on other applications and services across

Figure 58: Comparison of Ads & Tracking scores year-over-year results



the internet for advertising purposes. Additionally, industry norms have narrowed significantly since 2018, with a more consolidated range of scores in the interquartile range, but many applications and services are still providing a level of detail below industry norms and are considered extreme outliers below the Q1 score, indicated by dots in figure 58. Their policies should be updated to address these shortcomings. As explained in the California Privacy Rights Act (CPRA) section, it is expected that the median score of the Ads & Tracking concern category will increase in 2022 as more companies update their policies from "unclear" and "better" practices on selling data to "worse" practices that indicate they now sell users' data to third parties under the new CPRA law. Additionally, it is expected companies will also increase transparency on whether they use Third-party Tracking technologies on the product and Track Users on other applications and services across the internet.

Table 55: Ads & Tracking question response percentage point change from 2020 to 2021

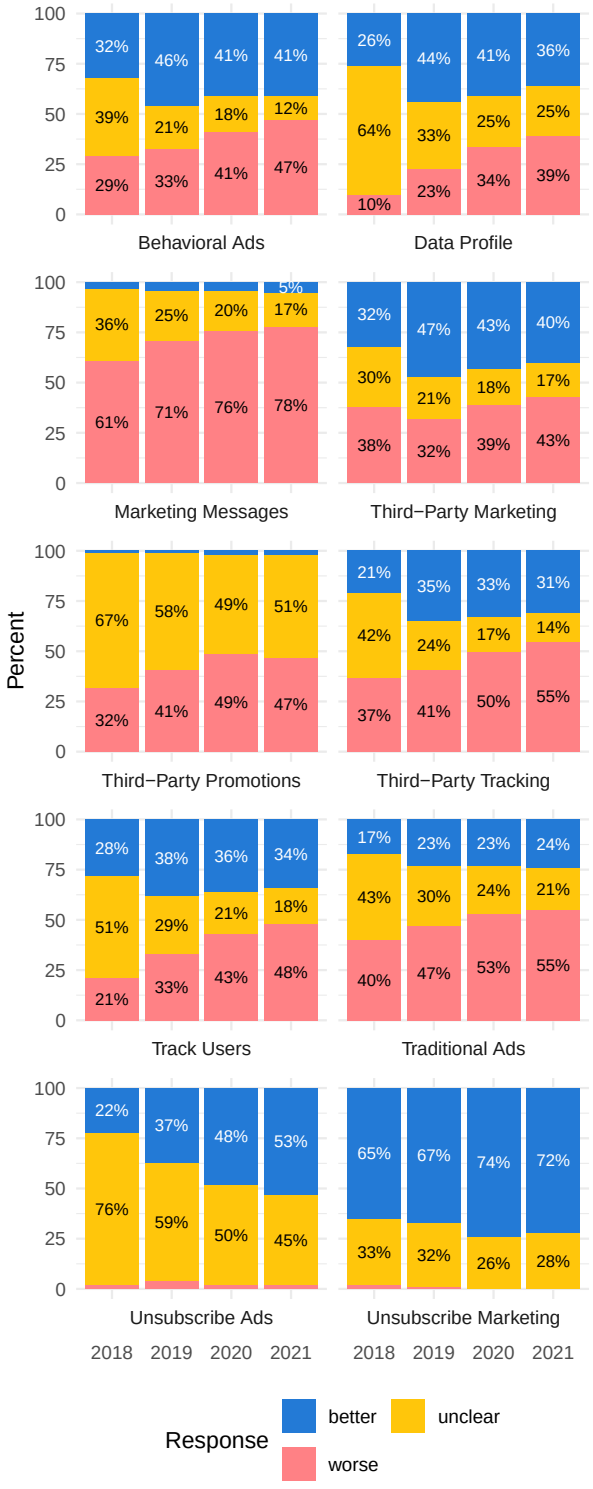
Question	"better"	"worse"	"unclear"
Behavioral Ads	0	6	-6
Data Profile	-4	6	0
Marketing Messages	0	2	-2
Third-Party Marketing	-2	4	-1
Third-Party Promotions	0	-1	0
Third-Party Tracking	-2	6	-3
Track Users	-2	4	-2
Traditional Ads	1	1	-2
Unsubscribe Ads	4	0	-5
Unsubscribe Marketing	-2	0	2

Although the Ads & Tracking concern category median score is stable at 60%, table 55 indicates some positive transparency changes and both positive and negative qualitative changes within the concern category that in the aggregate did not change the median score. For example, the Behavioral Ads, first-party Marketing Messages, Third-party Marketing, Third-party Tracking, and Track Users evaluation questions all indicate an increase from non-transparent or "unclear" policies to qualitatively "worse" practices that users are displayed targeted ads, sent third-party marketing communications, and tracked on other applications and services across the internet. In addition, the Data Profile evaluation question indicates a shift from "better" practices to "worse" practices of companies amassing a profile of a user based on their personal information collected from the product for monetization and advertising purposes.

However, there was also a shift from non-transparency or "unclear" to "better" practices with the Traditional Ads and Unsubscribe Ads evaluation questions, which indicates that as products include "worse" practices, they are also providing users with more ability to opt out or unsubscribe from targeted ads and receive only traditional or contextual advertising.

Ads are increasingly embedded along with tracking, making it difficult for a consumer to interpret how much of their privacy they are sacrificing to see various forms of advertising. Online ads have moved beyond the obviousness and obtrusiveness of banner

Figure 59: Ads & Tracking question response change year-over-year results.



ads flitting across the screen to a massive advertising and tracking ecosystem behind the simple transaction of buying an online product or service.[47] As a result, our process emphasizes the significant impact companies' decisions in this area have on individual user privacy.

Parental Consent

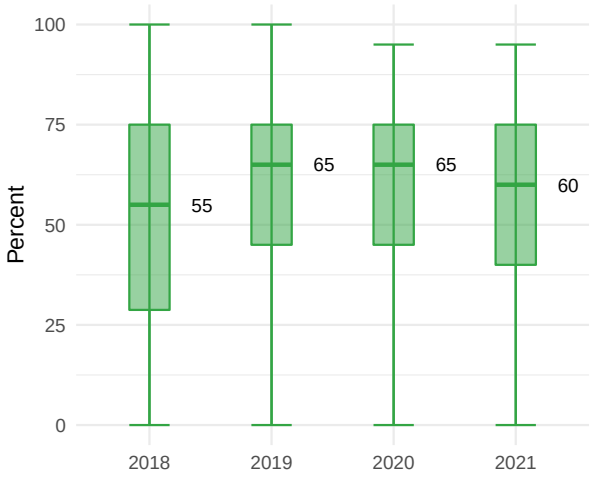
The Parental Consent concern category indicates whether the product is intended for children age 13 or under, and if a parent or guardian's verifiable consent is required before the collection, use, or disclosure of the child's personal information to an application or service. Figure 60 illustrates the Parental Consent median scores among all products evaluated. Table 56 compares and summarizes the Parental Consent concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

Table 56: Year-over-year results Parental Consent score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	29	55	51	75	100
2019	0	45	65	57	75	100
2020	0	45	65	58	75	95
2021	0	40	60	56	75	95

From the analysis of the 10 questions in the Parental Consent concern, we determined a median in 2021 of approximately 60%. This low median score is unexpected, given that these products are intended for children and students and that companies should disclose qualitatively "better" practices that they obtain parental consent for the collection, use, or disclosure of personal information from children using the product. The median score also appears to have decreased from 65% to 60%, which indicates that companies are shifting from disclosing "better" practices to non-transparent or "unclear" practices. This is likely a compliance-motivated change to avoid disclosing parental consent-related issues because children may no longer be the primary intended audience for the product. However, the decrease in the median score may also be attributed to policies not disclosing whether parents are an intended user of the product, because it is assumed they must be intended users if they are creating accounts with the product and also creating child profiles with the product for use by their children.

Figure 60: Comparison of Parental Consent scores year-over-year results



Since 2020 the Parental Consent category median score has decreased 7%, and has a stable minimum and maximum score. The lower quartile has also decreased since 2020. However, compared to 2018, applications and services evaluated in 2021 for the concern of Parental Consent indicate a 9% increase in median scores that translate to "better" transparent and qualitatively "better" practices of obtaining parental consent for the collection, use, or disclosure of personal information from children.

[47] *See* Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, and Phillipa Gill, *Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem*, 25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018, https://haystack.mobi/papers/ndss18_ats.pdf.

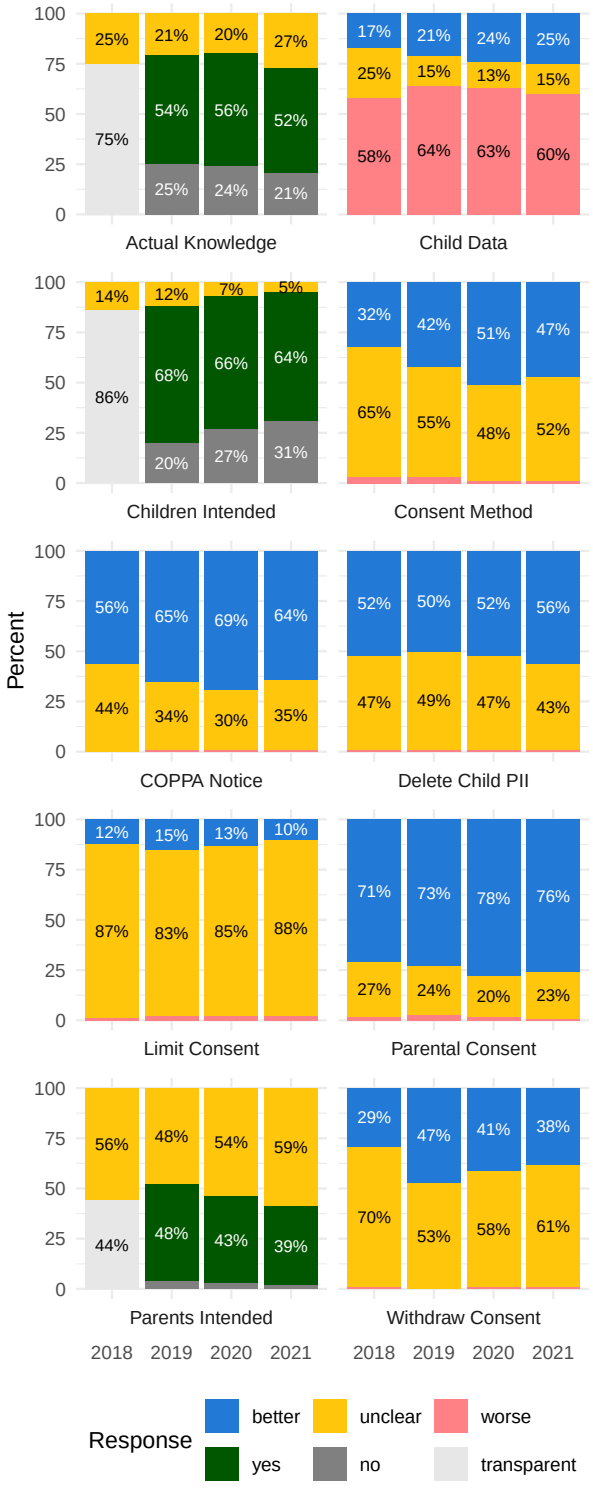
Table 57: Parental Consent question response percentage point change from 2020 to 2021

Question	"better"	"worse"	"unclear"	No	Yes
Actual Knowledge	NA	NA	7	-2	-4
Child Data	0	-4	3	NA	NA
Children Intended	NA	NA	0	3	-2
Consent Method	-3	-1	4	NA	NA
COPPA Notice	-5	0	4	NA	NA
Delete Child PII	4	0	-4	NA	NA
Limit Consent	-3	0	3	NA	NA
Parental Consent	-2	0	3	NA	NA
Parents Intended	NA	NA	5	-2	-4
Withdraw Consent	-3	0	4	NA	NA

The Parental Consent concern category median score decreased from 65% to 60%, and table 57 indicates significant negative transparency changes and negative qualitative changes within the concern category that decreased the median score. For example, the Actual Knowledge, Child Data, Consent Method, COPPA Notice, Limit Consent, Parental Consent, Parents Intended, and Withdraw Consent evaluation questions all indicate a decrease in transparent and "better" practices to non-transparent or "unclear" policies that do not discuss whether children's privacy is protected by the product by obtaining informed consent from parents for the collection, use, or disclosure of children's personal information.

This finding is unexpected given that the products used in this report are among the most popular products used by children and students. Perhaps companies that shifted to non-transparency in the Parental Consent concern assume they do not need to obtain parental consent if they disclose their service is not intended for children or students. However, the Children Intended evaluation question indicates that 64% of products disclose their products are intended for children, with 5% remaining "unclear." In addition, companies may have removed references in their policies to children as an intended audience and obtaining parental consent as a compliance-motivated decision. Companies may be changing their policies to disclose the product is neither directed nor targeted to children under 13 years of age to avoid potential liability under

Figure 61: Parental Consent question response change year-over-year results.



COPPA if the product also displays targeted advertising or tracks users on other applications and services across the internet. COPPA requires applications and services to obtain parental consent only where the company 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, with parents as intended users creating child profiles as a method of providing consent, because these products would likely appeal to children under the age of 13, which take into account several factors, as described in the Intended Users section.

Lastly, the Delete Child PII evaluation question indicates a shift from "unclear" to "better" practices of companies disclosing that they will delete any personal information of children collected by the product if they obtain actual knowledge the user providing the information is a child. This shift aligns with the previously stated assumption that the industry in 2021 may be changing their policies to be less transparent on the issue of whether children are an intended audience of the product. This change could be the result of companies not disclosing whether children are intended to allow for plausible deniability that the company does not know whether any of its users are children to avoid compliance obligations under COPPA.

This has serious implications that children's privacy has actually decreased across the industry since 2020 if stronger privacy protections are not put in place. Among products evaluated over all four years, the trends are largely the same since 2018.

School Purpose

The School Purpose concern category indicates whether the product collects data from K-12 students and how the company follows Federal and State legal obligations for the privacy and security of that educational information. Figure 62 illustrates the School Purpose median scores among all products evaluated. Table 58 compares and summarizes the School Purpose concern score minimum, maximum, median, mean, Q1 (point between the first and second quartiles), and Q3 (point between the third and fourth quartiles).

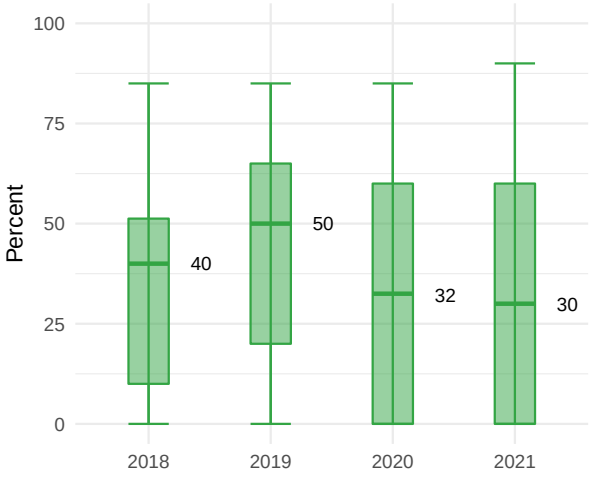
Table 58: Year-over-year results School Purpose score descriptive statistics

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	10	40	36	51	85
2019	0	20	50	42	65	85
2020	0	0	32	34	60	85
2021	0	0	30	33	60	90

From the analysis of the 10 questions in the School Purpose concern, we determined a median score in 2021 of approximately 30%, which is one of the lowest median scores across all evaluation concerns. This low median score is unexpected, given that these products are intended for children and students, and companies should disclose qualitatively "better" practices that students are intended users and the product is intended for use in a K-12 school or district given the majority of the products in this report are used by students. Educators and parents can help improve the ecosystem by putting pressure on companies that do not disclose whether their products are intended for students by only choosing to use products with students in their K-12 schools and districts that transparently disclose in their policies that students are the intended audience and that also have strong student data privacy protections. The median score also appears to be stable at 30% which indicates that School Purpose-related industry practices are not getting "better" or "worse" and that companies are still not disclosing "better" practices about protecting student data. These would include the school obtaining parental consent on behalf of parents, or whether educational records are created with the product, or whether additional student data privacy agreements with schools or districts are available.

Since 2020 the School Purpose category median score, and other descriptive statistics, have remained stable. However, the lower whisker has the same score as the minimum score, which means that variability is very low on the low end of the distribution. Compared to 2018, applications and services evaluated in 2021 for the concern of School Purpose indicate a 25% decrease in median scores that translate to "worse" transparent and qualitatively "worse" practices of protecting student data privacy. This lack of transparency by the majority of products regarding the School Purpose concern could create confusion for parents, teachers, schools, and

Figure 62: Comparison of School Purpose scores year-over-year results



districts about whether additional compliance obligations would be applicable to the application or service for students under 18 years of age, and in many of those cases means these products should not be used in an educational setting without additional contracts put in place to ensure students are protected. Some of these shifts in response data are due to our shift in products evaluated, especially in 2020. With the exception of Directory Information, which had a chi-square p-value of 0.07, every question in this concern had a chi-square p-value lower than 0.003 – well below our threshold of 0.05 – indicating that 2020 response changes were likely indicative of our change in products evaluated rather than any large shift in industry practices. See Product Population Demographics for a more detailed analysis and an interpretation of the chi-square p-values.

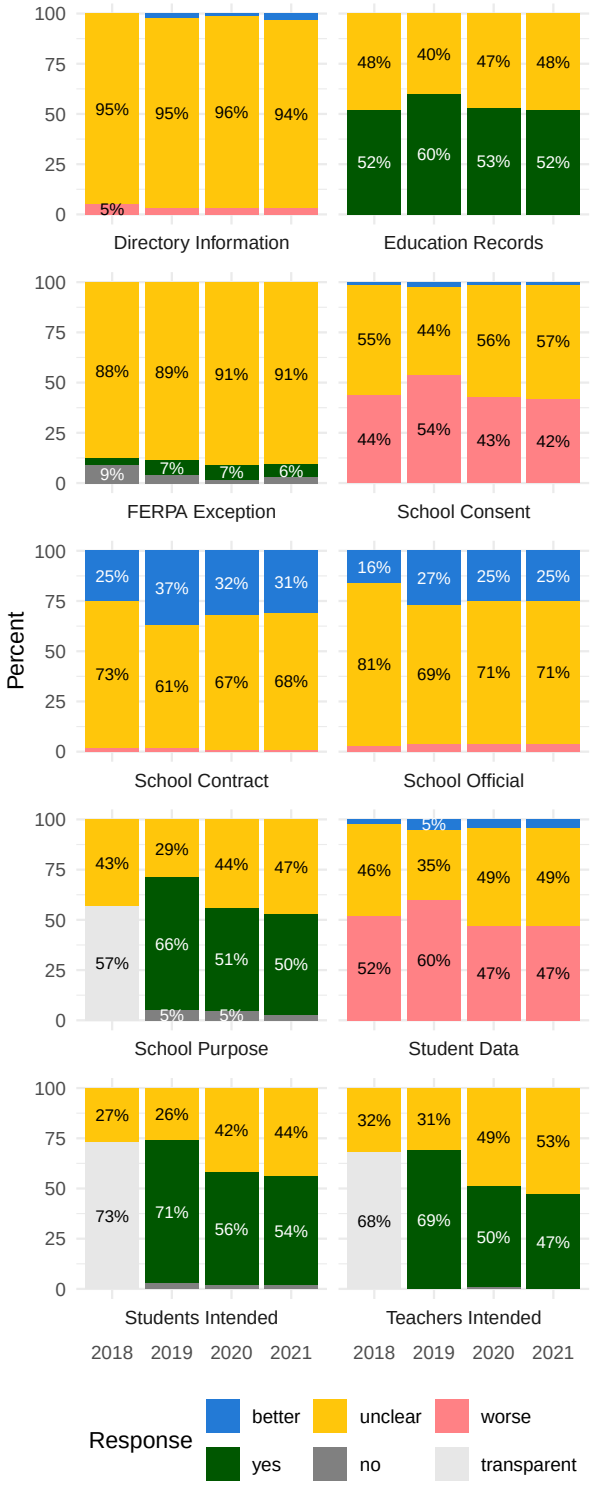
Table 59: School Purpose question response percentage point change from 2020 to 2021

Question	"better"	"worse"	"unclear"	No	Yes
Directory Information	1	0	-2	NA	NA
Education Records	NA	NA	1	NA	-1
FERPA Exception	NA	NA	1	1	-1
School Consent	0	-2	1	NA	NA
School Contract	-1	0	0	NA	NA
School Official	-1	0	1	NA	NA
School Purpose	NA	NA	4	-3	0
Student Data	0	0	0	NA	NA
Students Intended	NA	NA	2	0	-2
Teachers Intended	NA	NA	3	-1	-4

The School Purpose concern category median score is stable at 30%, but table 57 indicates some negative transparency changes at the individual question level. However, these losses in transparency did not significantly impact the median score. For example, the School Consent, School Purpose, Students Intended, and Teachers Intended evaluation questions all indicate an increase in non-transparent or "unclear" policies that do not discuss whether students or teachers are intended users of the product or whether the product is intended to be used in K-12 schools or districts.

Some of these shifts are certainly due to our change in products evaluated since 2018 that include fewer products that would be traditionally classified as only for use with students in K-12 schools and districts. Additionally, perhaps the low median score and the shift to non-transparency with questions in the School Purpose concern is the result of companies assuming they do not need to disclose they are intended for students because the product is intended for a general or mixed audience. However, due to safety concerns related to COVID-19 in 2020 schools and districts shifted to fully online or hybrid learning, in some cases overnight with the use of many new applications and services that may have not been fully vetted or appropriate contracts put in place to ensure students were properly protected. In some cases, products that may not have been intended for students or educational purposes were used due to expediency and concerns about learning loss. For example, the videoconferencing

Figure 63: School Purpose question response change year-over-year results.



service Zoom was originally designed for consumer and business customers, but the company saw explosive growth in the first few months of 2020, expanding their userbase to more than 300 million active participants. These included educators, children, and students who were not originally intended users of the product, so educational contexts were not appropriately considered. To put this in context, Zoom said they had only about 10 million paid and free daily active participants at the end of December 2019. Increasing demand by 30 times in such a short time period and during a global pandemic can understandably put a strain on any product – especially one that saw explosive growth with students using their product for educational purposes in ways they never intended.

Alternatively, when the product is purchased by a school or district, the company may enter into a student data privacy School Contract to better protect a student's data collected by the product. Therefore, companies may assume its publicly available privacy policy does not apply to students when used in a K-12 school or district, so their public policy remains non-transparent or "unclear." Accordingly, a contract or student data privacy agreement with a local education agency[48] 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, when the product is "unclear" whether students are intended users, or when the school or district needs to clearly define the company's compliance obligations and places the company under the direct control of the educational institution. Companies that disclose that their applications or services are intended for students and are primarily designed, marketed, and intended for preschool or K-12 School Purpose, but are "unclear" on questions in this concern may be "unclear" because they believe that their supplemental contracts with schools and districts sufficiently protect student data and satisfy any required compliance obligations.

Negotiated student data privacy agreements serve to fill the 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

[48] A Local educational agency or LEA means a public board of education or other public authority legally organized within a state for either administrative control or direction of public elementary schools or secondary schools in a city, county, township, or school district.

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 that 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 that 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 companies 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 students will be protected in order to meet their expectations of privacy based only on the publicly available privacy policy. As a result, only sophisticated, large, and well-resourced school districts are likely to be in a position to secure additional protections afforded by a negotiated agreement that supersedes or supplements the publicly available privacy policy.

Products evaluated all four years

Table 60 compares the previous School Purpose concern scores to the smaller population of products that were only evaluated over all four years. This smaller population size excludes new products added in 2019, 2020, and 2021, which may include a higher percentage of products likely classified as kids' tech than traditional edtech where companies disclose the product is primarily intended only for students in K-12 schools and districts.

Table 60: Year-over-year results School Purpose score descriptive statistics products evaluated all four years

	Min.	Q1	Median	Mean	Q3	Max.
2018	0	20	40	39	58	85
2019	0	28	50	45	65	85
2020	0	25	55	47	70	85
2021	0	25	60	48	70	90

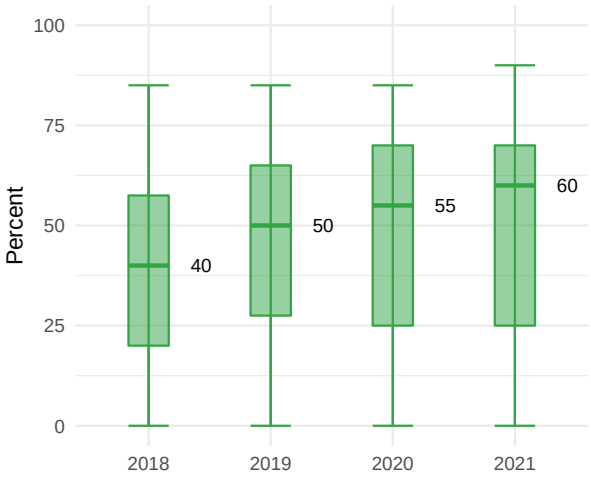
For products that were evaluated over all four years and more likely to be considered for use or used in the classroom, figure 64 indicates an increasing median score since 2018, from 40% to 60%. In contrast to the larger population of products that include both edtech and kids' tech with a median score that decreased to 30%, the smaller population of edtech products indicate an increasing median score, which is significantly higher than the median score for the larger population. This is expected, given that the population of products added since 2018 included a greater percentage of kids' tech products with less transparency on student data privacy-related issues.

The higher median score of the School Purpose concern category for products evaluated over all four years indicates a consistent trend that products more likely to be considered for use or used in the classroom are improving year over year with increasing transparency on issues related to student data privacy.

However, the median score is still too low to adequately protect students given the smaller population size of the most popular products primarily used or considered for use in K-12 schools and districts.

The School Purpose concern category median score for products evaluated all four years increased from 40% to 60%, and table 61 indicates positive transparency changes within the concern category that increased the median score. In contrast to the larger population of kids' tech (including products primarily used or considered for use in the classroom) that indicates an overall decrease in transparency with "unclear" practices, products that are more likely to be considered for use or used in the classroom

Figure 64: Comparison of School Purpose products evaluated all four years scores year-over-year results



increased their transparency across multiple issues in the School Purpose category.

For example, the Directory Information, FERPA Exception, School Purpose, Students Intended evaluation questions all indicate an increase in transparent or "better" practices. This trend is expected given these edtech products are the most popular products with students in K-12 schools and districts. In addition, these products also increased transparency on the Student Data and School Consent evaluation questions from "unclear" to "worse" practices, which indicates these companies are increasing their transparency that the product collects data from students and they may obtain parental consent for the collection, use, and disclosure of that data from the school or district.

This shift in transparency is promising for this subpopulation of products evaluated all four years because it indicates that products primarily intended for students in K-12 schools and districts have been improving their privacy practices year over year. This positive trend is likely in response to the increase of state-by-state student data privacy laws since 2018, which required schools and districts to ensure student data privacy agreements or contracts are put in place between edtech companies and the local educational agency to better protect student data privacy. This trend is also likely the result of increased student data privacy awareness of parents and educators, who put financial pressure on the edtech marketplace of companies by choosing to purchase only better privacy-protecting products for students.

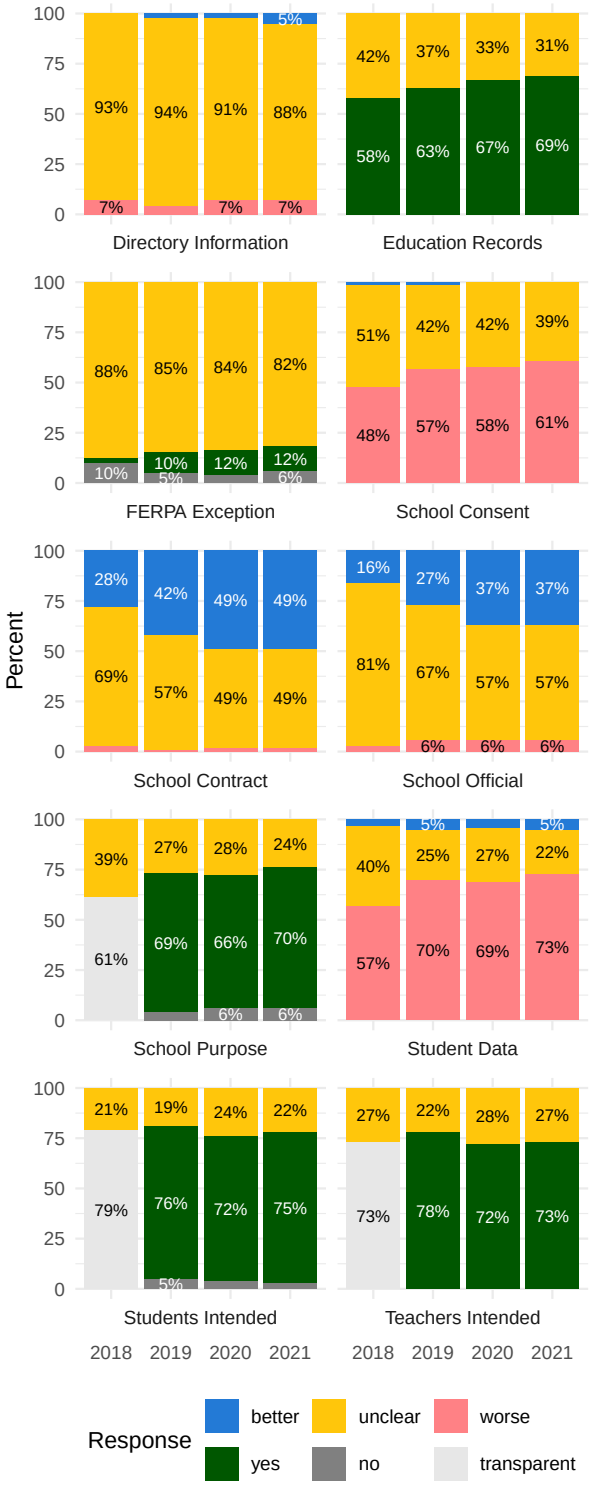
Our evaluation process also plays a contributing factor here. As more districts are aware of our process and the work we have already done, they can request that companies more clearly define the details that need to be covered in their policies.

In some cases, we work closely with companies who have received requests from districts to improve their practices, and in many of these cases the updated publicly available policies address issues raised from our evaluations. The advantages of this process, rather than a custom contract for each school or district, are less work for everyone and a more equitable solution because the baseline privacy protections are available to all users regardless of their respective ability and resources to navigate the complex realities of contract law at the intersection of protecting student data privacy. Edtech companies that fail to keep pace with the industry, and their competitors with better baseline privacy protections, may soon find they are unable to compete in an evolving marketplace where privacy continues to become an even more important and competitive differentiating factor.

Table 61: School Purpose question response percentage point change from 2020 to 2021 products evaluated all four years

Question	"better"	"worse"	"unclear"	No	Yes
Directory Information	3	0	-3	NA	NA
Education Records	NA	NA	-2	NA	2
FERPA Exception	NA	NA	-2	2	0
School Consent	NA	3	-3	NA	NA
School Contract	0	0	0	NA	NA
School Official	0	0	0	NA	NA
School Purpose	NA	NA	-4	0	4
Student Data	0	4	-5	NA	NA
Students Intended	NA	NA	-2	-1	3
Teachers Intended	NA	NA	-1	NA	1

Figure 65: School Purpose question response change year-over-year results products evaluated all four years.



CONCLUSION

The State of Kids' Privacy Report 2021 is a snapshot of where we are at a moment in time. The report describes our privacy evaluation process, demonstrates the breakdown of the 10 most important privacy concerns for consumers, parents, and educators, and highlights where the industry can do better. The State of Kids' Privacy Report indicates a widespread lack of transparency and failure to protect children and students with better practices that apply to all users of a product.

Now that we know what's wrong across the industry, let's work together to write a prescription to fix the system. The purpose of this critically important research is to better inform policymakers of direct evidence of the privacy practices, as publicly provided by companies, regarding the most popular applications and services that impact children and students and are used at home and in the classroom every day. The findings in this report should serve as a wake-up call for state and federal legislators that the state of kids' privacy is so poor that stronger privacy laws and enforcement are needed to better protect the privacy of our children and students.

In addition, the findings in this report should also serve to provide regulators with the information they need to make better informed decisions in the pursuit of more focused and meaningful enforcement of products potentially violating federal or state privacy laws, or engaging in unfair or deceptive practices. In some cases the use of these products may be unavoidable by children and students, requiring even further diligence, protection, and enforcement to ensure their data and privacy are appropriately protected

We need the industry to step up and do more to protect kids from the current reality in which kids' tech and edtech products are actively engaging in more data collection and data monetization than ever before.

The in-depth results described in this report are one of a kind in that they quantify and qualify a field of study that heretofore has been a matter of conjecture. Privacy, especially children's privacy, has moved beyond its speculative early days in which practitioners hypothesized about which privacy-protective practices would work to effect positive change in the industry. We don't know all of the answers yet, but we do know most of the questions. This report is where we asked the difficult questions and then formulated the answers by reading and examining the actual privacy policies of 200 products used by kids at home and students in the classroom. What we found generally was not good, but we did find a way to communicate the efforts that companies made towards compliance and transparency. If a product is rated highly, achieving both a Pass rating and a high overall score in our privacy evaluation process, it is because the product is a comparatively better privacy "bargain" than one that receives a *Warning* rating and/or a lower score. Our evaluation process aims to shed light on the inscrutable world of endless pages of legalese and technical descriptions. When parents and educators see these ratings, it is our hope that they can follow a clear path toward choosing better products for themselves, and their children and students; regardless of the obfuscations and challenges that lie ahead.

Privacy is an ongoing process with constantly changing expectations, at the intersection of ever-changing people and technology, rather than a clear goal that can be definitively achieved and laid to rest. The evaluation process described in this report is a combination of the trial-and-error work done by a team of experts, and reflects a methodical and intentional approach to evaluating privacy policies at the highest possible standard of quality and accuracy using what we know about technology, law, best practices, people, child development, and the operation of markets.

As we discover new products, we enter them into our systems, not only to understand how the product holds up on privacy but also to continually test our systems against these products to see what works and what does not. We frequently interact with app developers and marketers to ask what they can do to improve their products' privacy and transparency practices, and what they can suggest to improve our systems and our methodologies for communicating our privacy evaluation results and ratings to a wide range of stakeholders.

This work continues on multiple fronts to address almost constant technological change, with new products and devices for kids and students entering the marketplace daily. Beyond this report, we continue to update all our evaluations whenever we see a company's policy has changed and post them on our

website for free to facilitate global availability and ease of access for everyone. In addition, we engage with hardware devices as well as software applications and services, and have started to dive into the world of Artificial Intelligence and Machine Learning to increase the speed, accuracy, and consistency of our evaluation systems.

Future Work

Our work contributes to existing bodies of research within the fields of privacy, consumer advocacy, human-computer interaction, policy, and other related subjects such as IoT (Internet of Things), streaming devices, and observational testing of advertising and tracking technologies.

Device Research

Beyond apps and websites, the digital landscape is changing quickly, with apps now available for use across tablets or smartphones and other devices like smart TVs, voice assistants, and more. Our recently published report on the privacy of streaming apps and devices[49] covers our latest work reviewing the privacy policies of the top 10 streaming apps and represents one area of future work we plan to pursue. We are similarly interested in the privacy of VR/AR (Virtual or Augmented Reality) devices, as well as exploring other IoT devices that may put kids' or students' data at risk. At present we are beginning to pursue our own research into these different device types, and are interested in collaborating with researchers investigating similar topics to better achieve our goals of helping consumers, parents, and educators understand the privacy implications of the products they use.

Understanding AI and AdTech

Machine learning, a subfield of artificial intelligence (AI), applies computer algorithms to a dataset in order to identify patterns and iteratively "learn" from new data. It is a powerful tool that can be used to enhance education, but as with any robust technology, it must be used and considered carefully. We're making advances in this area to enhance our existing systems and expand the reach of these systems beyond the labor resources of our team of engineers and evaluators.

We have two main goals in researching AI and AdTech. Firstly, we want to know more about the student and kids' technologies that use AI. Parents and educators should be equipped with knowledge that helps them decide whether an app or software is not only safe for their kids to use, but also if the machine learning model used fairly represents student outcomes with minimal bias. Parents and educators should also be empowered to test the AI models themselves and be given enough context to evaluate privacy or ethical risks. Secondly, we want to see if AI is effective for evaluating privacy policies. Our evaluations require ample time and manual labor to complete, and our research into NLP (Natural Language Processing) and transformers[50] for supervised classification may help us expedite the evaluation process and scale our evaluations to include more products. This will allow us to provide parents and educators with more information on more apps and services, without requiring a deep understanding of "legalese."

These two goals further our mission of empowering people with regards to the privacy decisions they must make for their children, students, and school districts, whether through educating parents and educators or by using AI as a tool ourselves.

Continuing Research and Policy Work

We engage with our systems to improve privacy practices, and we work with individuals in the field to improve privacy policies. However, it's worth mentioning in this data-focused process that words still matter. The legislative language that emerges from our U.S. federal, state, and international authorities continue to affect what is communicated about privacy in companies' privacy policies. Transparency is necessary, of course, but our experience with evaluating privacy policies is that transparency is not sufficient in and of itself to protect privacy, because whether a product's practices are privacy-protecting or privacy-regressive matters.

Further research should attempt to duplicate and enhance our results by looking at updating the questions to encompass more perspectives. In addition, researchers may find it fruitful to examine our data

[49] *See* Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). Privacy of Streaming Apps and Devices: Watching TV that Watches Us. San Francisco, CA: Common Sense Media, https://www.commonsensemedia.org/research/privacy-of-streaming-apps-and-devices-2021.

[50] *See* Devlin, J.; Chang, M.-W.; Lee, K.; and Toutanova, K. 2018. *Bert: Pre-training of deep bidirectional transformers for language understanding*. arXiv:1810.04805v2.

to come to other conclusions and make recommendations for privacy by design. Additional work is also necessary to improve the means of communicating privacy practices to parents, teachers, students, and consumers as the current reality leaves many in a position, even if they can navigate the complex reality of privacy policies, where they are unable to fully understand the implications of existing and evolving privacy practices.

Privacy for everyone, not just kids, should be the default assumption in privacy by design. To accomplish that ideal, we encourage legislators, regulators, and their policy advisors to focus on where their actions will have the largest impact. In addition to improved and more meaningful enforcement for companies that fall below user expectations and industry norms, we should look at the companies with the biggest impact on the privacy of children and students, and require them to set higher standards for the entire marketplace. And when we find companies who are setting their privacy standards high, we open the possibility that more companies will aspire to reach those standards and differentiate themselves from their competitors and the state of the industry.

APPENDIX

Statute Questions

Below are each statute analyzed in this report with links to respective related questions.

GDPR

The 61 questions related to GDPR in our set of evaluation questions are as follows: Vendor Contact, Quick Reference, Children Intended, Teens Intended, Adults Intended, Collect PII, PII Categories, Geolocation Data, Health Data, Behavioral Data, Sensitive Data, Usage Data, Collection Limitation, Data Shared, Sharing Purpose, Third-Party Analytics, Exclude Sharing, Data Acquired, Third-Party Categories, Data De-identified, De-identified Process, Third-Party Limits, Purpose Limitation, Data Purpose, Context Notice, Context Consent, Collection Consent, Complaint Notice, Opt Out Consent, Disclosure Request, Disclosure Notice, Access Data, Restrict Access, Maintain Accuracy, Data Modification, Modification Process, Modification Notice, Retention Policy, Retention Limits, Deletion Purpose, User Deletion, Deletion Process, Deletion Notice, User Export, Contractual Limits, Verify Identity, Security Agreement, Reasonable Security, Transit Encryption, Storage Encryption, Data Control, Breach Notice, Security Audit, Data Profile, Unsubscribe Marketing, School Contract, Parental Consent, Withdraw Consent, Privacy Badge, GDPR Jurisdiction, GDPR Role

COPPA

The 71 questions related to COPPA in our set of evaluation questions are as follows:

Vendor Contact, Children Intended, Teens Intended, Adults Intended, Parents Intended, Collect PII, PII Categories, Geolocation Data, Health Data, Behavioral Data, Usage Data, Child Data, Collection Limitation, Data Shared, Data Categories, Sharing Purpose, Third-Party Analytics, Third-Party Research, Third-Party Marketing, Sell Data, Third-Party Providers, Third-Party Roles, Vendor Combination, Data De-identified, De-identified Process, Third-Party Limits, Combination Limits, Purpose Limitation, Combination Type, Collection Consent, Access Data, Restrict Access, Review Data, Maintain Accuracy, Modification Process, Deletion Purpose, Account Deletion, Deletion Process, Transfer Data, Contractual Limits, Verify Identity, Security Agreement, Reasonable Security, Data Control, Safe Interactions, Unsafe Interactions, Share Profile, Visible Data, Filter Content, Moderating Interactions, Traditional Ads, Behavioral Ads, Third-Party Tracking, Track Users, Data Profile, Marketing Messages, Third-Party Promotions, Unsubscribe Ads, Actual Knowledge, COPPA Notice, Restrict Account, Restrict Purchase, Safe Harbor, Parental Consent, Limit Consent, Withdraw Consent, Delete Child PII, Consent Method, Internal Operations, COPPA Exception, Law Enforcement

FERPA

The 36 questions related to FERPA in our set of evaluation questions are as follows: Students Intended, Teachers Intended, Collect PII, Geolocation Data, Health Data, Behavioral Data, Usage Data, Lunch Status, Student Data, Collection Limitation, Data Shared, Third-Party Research, Data De-identified, De-identified Process, Third-Party Limits, Disclosure Request, Disclosure Notice, Restrict Access, Review Data, Modification Process, Retention Limits, Account Deletion, Deletion Process, Verify Identity, Security Agreement, Reasonable Security, Data Control, Track Users, Education Records, School Contract, School Official, Parental Consent, Delete Child PII, FERPA Exception, Directory Information, Law Enforcement

CPRA

The 58 questions related to CPRA in our set of evaluation questions are as follows: Effective Changes, Collect PII, PII Categories, Geolocation Data, Health Data, Behavioral Data, Sensitive Data, Usage Data, Collection Limitation, Data Shared, Data Categories, Sharing Purpose, Third-Party Analytics, Third-Party Research, Third-Party Marketing, Sell Data, Data Acquired, Data Misuse, Third-Party Providers, Third-Party Roles, Third-Party Categories, Third-Party Policy, Data De-identified, De-identified Process, Third-Party Limits, Combination Limits, Purpose Limitation, Data Purpose, Context Notice, Collection Consent, Opt Out Consent, Disclosure Request, Review Data, Data Modification, Modification Process, Modification Notice, Retention Policy, Retention Limits, Deletion Purpose, User Deletion, Deletion Process, Deletion Notice, User Export, Transfer Data, Verify Identity, Reasonable Security, Employee Access, Breach Notice, Traditional Ads, Behavioral Ads, Third-Party Tracking, Track Users, Data

Profile, Marketing Messages, Actual Knowledge, Education Records, Law Enforcement, GDPR Role

CalOPPA

The 26 questions related to CalOPPA in our set of evaluation questions are as follows: Effective Date, Change Notice, Method Notice, Review Changes, Effective Changes, Services Include, Vendor Contact, Collect PII, PII Categories, Geolocation Data, Usage Data, Exclude Sharing, Data Acquired, Authorized Access, Third-Party Collection, Third-Party Categories, Access Data, Review Data, Data Modification, Modification Process, User Deletion, Third-Party Tracking, Track Users, Unsubscribe Ads, DoNotTrack Response, DoNotTrack Description

SOPIPA

The 35 questions related to SOPIPA in our set of evaluation questions are as follows: Students Intended, Teachers Intended, Geolocation Data, Health Data, Usage Data, Student Data, Data Shared, Sharing Purpose, Third-Party Analytics, Third-Party Research, Third-Party Marketing, Sell Data, Third-Party Providers, Third-Party Roles, Third-Party Combination, Data De-identified, De-identified Process, Third-Party Limits, Purpose Limitation, Account Deletion, Deletion Process, User Export, Transfer Data, Contractual Limits, Security Agreement, Reasonable Security, Data Control, Behavioral Ads, Third-Party Tracking, Track Users, Data Profile, Marketing Messages, Third-Party Promotions, School Purpose, Law Enforcement

Pupil Records

The 15 questions related to Pupil Records in our set of evaluation questions are as follows: Teachers Intended, Purpose Limitation, Data Ownership, Review Data, Modification Process, Deletion Purpose, User Export, Security Agreement, Reasonable Security, Employee Access, Data Control, Breach Notice, School Contract, School Official, Parental Consent

Evaluation Questions

The following full evaluation questions are used in our evaluation framework to generate the overall full score and concern category scores. Each individual evaluation question below indicates the percentage of question responses to our full evaluation of the company's privacy policies over the past four years. Most evaluation questions have a "better" or "worse" qualitative component that has been determined through interviews with consumers, parents, educators, academics, privacy experts, and policymakers about their expectations of privacy.

Each evaluation question's qualitative component is also applied against a privacy risk assessment framework that considers whether the collection, use, or disclosure of personal information from any user of the product increases or decreases their privacy risk.[51] All of the full evaluation questions attempt to create a comprehensive assessment of all the concerns a product's privacy policy should disclose that could apply to any intended user. The evaluation questions also attempt to balance a user's risk against a company's risk where if a product's polices disclose a "worse" practice that increases risk for a user that is unavoidable, there are other related evaluation questions that a product can disclose with "better" practices to mitigate risk, transfer risk, avoid risk, or accept the risk.

In addition, many evaluation questions do not have a "better" or "worse" qualitative component because they are complex and therefore only indicate "Yes" or "No" in regards to transparency about the specified practice described in the question. A complex question indicates it may be, generally speaking, difficult to determine whether a practice is "better" or "worse". For complex questions, more specific context is necessary and overall risk may depend on the type of user of the product, or there may also be an unavoidable practice for the majority of products – such as sharing data – that could increase or decrease risk for the user depending on the purpose for which their data is used. Alternatively, some questions do not have a qualitative component and instead merely indicate that a practice is or is not happening. The full evaluation questions are listed below in the order in which they appear in our

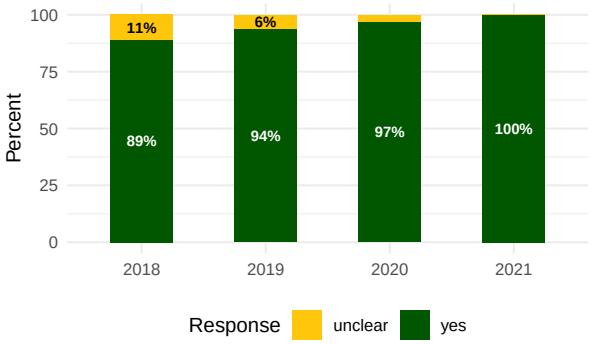
[51] NIST, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (Jan. 16, 2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

evaluation process, which also aligns with the Fair Information Practice Principles (FIPPs).[52]

Effective Date

The Effective Date evaluation question indicates whether the current version or effective date of the policies is clearly disclosed. The effective date is important to disclose because it provides notice to users if, and when, the terms of a product changed. If a policy's effective date changes, that could also mean that the data collection practices of the product may also have changed and could impact a user's privacy. This evaluation question does not have a "better" or "worse"' qualitative component. This question is also included in our basic evaluation process.[53]

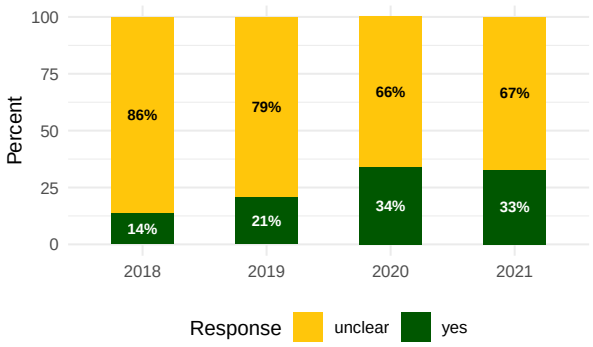
Figure 66: Effective Date: Do the policies clearly indicate the version or effective date of the policies?



Change Log

The Change Log evaluation question indicates whether a public archive or summary of the recent policy changes is available for review. Often it is not clear to a user what additions or deletions were actually made to a policy when the version or effective date changes. Rather than asking users to reread the entire policy and compare the differences between versions, it is better to summarize or indicate what practices changed since the last version that may impact the user's privacy; users can then make a better informed decision whether to continue using the product. This evaluation question does not have a "better" or "worse"' qualitative component.

Figure 67: Change Log: Do the policies clearly indicate a changelog or past policy versions available are for review?



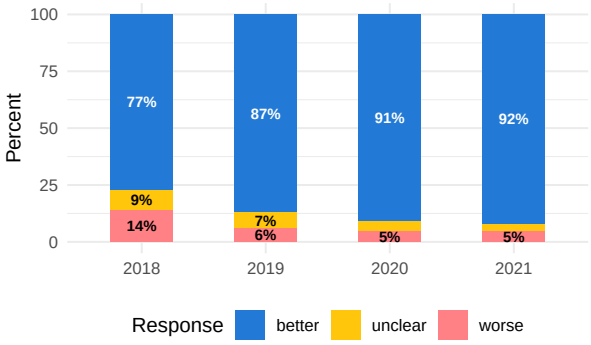
[52] Federal Trade Commission (FTC), *Privacy Online: Fair Information Practices in The Electronic Marketplace* (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[53] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(4).

Change Notice

The Change Notice evaluation question indicates whether or not notification will be provided to users about any changes made to the policies that result in a new version or new effective date of the policies. A company should provide notice to users when they change their policies because the changes may impact the collection or use of a user's data and may change their decision whether to continue using the product. A "better" response to this evaluation question indicates the product does provide notice to users about any changes made to the policies.[54]

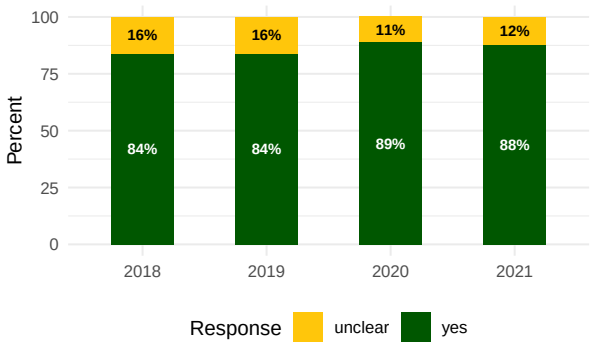
Figure 68: Change Notice: Do the policies clearly indicate whether or not a user is notified if there are any material changes to the policies?



Method Notice

The Method Notice evaluation question indicates how users will be directly notified of changes to the company's policy. A company is required to describe the process by which they notify users of changes to policies and obtain consent, which need to be more prominent than simply changing the version or effective date of the policies. Companies need to describe whether they provide adequate notice to users through email, postal mail, mobile notifications, or prominent banners on the website login page or upon launch of a mobile application. This evaluation question does not have a "better" or "worse" qualitative component.[55]

Figure 69: Method Notice: Do the policies clearly indicate the method used to notify a user when policies are updated or materially change?



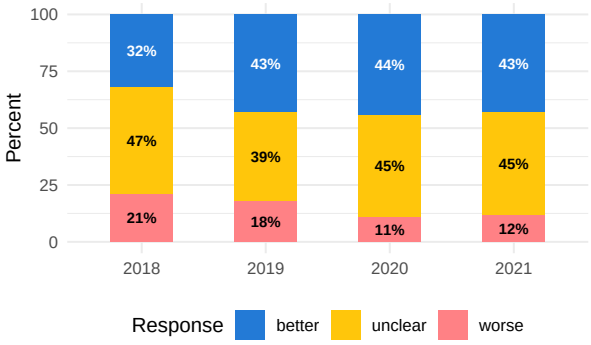
[54] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(3).

[55] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(3).

Review Changes

The Review Changes evaluation question indicates the time frame for notification prior to changes to the policies coming into effect. A company should provide adequate time for a user to review any changes to the policies – such as 30 days – to allow the user to make a better informed decision whether to continue using the product. A "better" response to this evaluation question indicates the product does provide a time frame for notification prior to changes to the policies coming into effect.[56]

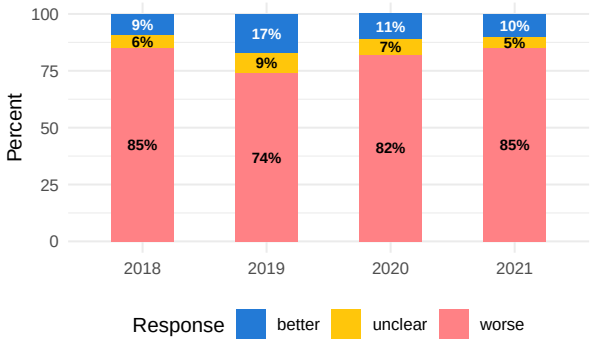
Figure 70: Review Changes: Do the policies clearly indicate whether or not any updates or material changes to the policies will be accessible for review by a user prior to the new changes being effective?



Effective Changes

The Effective Changes evaluation question indicates whether or not changes to a company's policies are effective immediately without prior review, and whether use of the service by the user indicates consent to any changes. A company should not make changes to its policies that impact the collection or use of a user's personal information without clear notice and informed consent from a user. A "better" response to this evaluation question indicates the company's policies are not effective immediately without prior review.[57,58]

Figure 71: Effective Changes: Do the policies clearly indicate whether or not any updates or material changes to the policies are effective immediately and continued use of the product indicates consent?



[56] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(3).

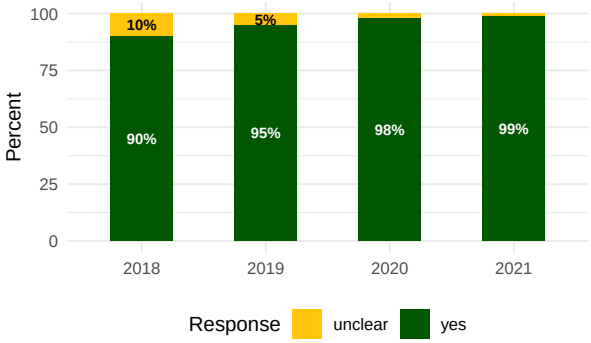
[57] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(3).

[58] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ad)(2)(C).

Services Include

The Services Include evaluation question indicates which websites, apps, or services make up the scope of the company's policies. A company should clearly define what products are covered under the policies so users have clear notice what data collection and use practices apply to which products they use. This evaluation question does not have a "better" or "worse" qualitative component.[59]

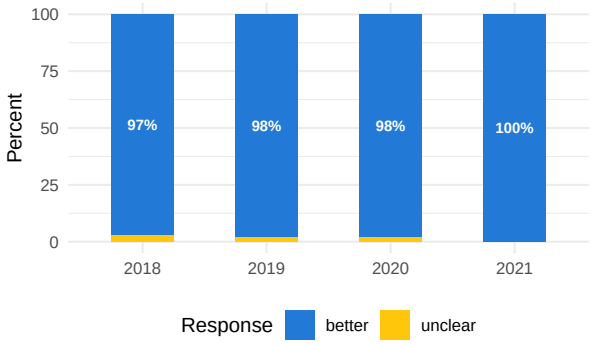
Figure 72: Services Include: Do the policies clearly indicate the products that are covered by the policies?



Vendor Contact

The Vendor Contact evaluation question indicates whether the contact information of the company is provided for users to ask questions and receive answers about the company's privacy practices or exercise their privacy rights by email, phone number, postal mail, or webform submission. A "better" response to this evaluation question indicates the product does provide contact information for the company.[60,61,62,63,64]

Figure 73: Vendor Contact: Do the policies clearly indicate whether or not a user can contact the vendor about any privacy policy questions, complaints, and material changes to the policies?



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

[60] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(1).

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

[62] *See* California Electronic Commerce Act, Cal. Civ. Code § 1789.3.

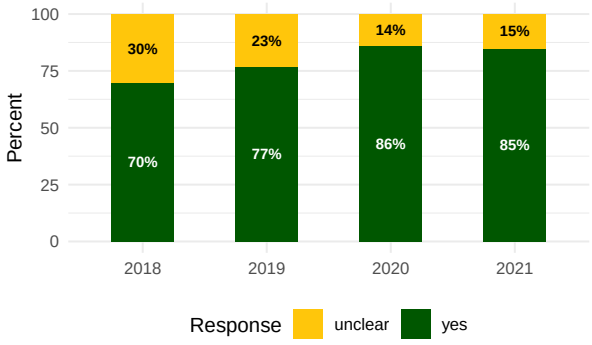
[63] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art.

[64] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(a).

Quick Reference

The Quick Reference evaluation question indicates whether a company's privacy principles, easy-to-read summary, table of contents, or explanations of the practices of the privacy policy are disclosed. A company should provide clear notice of the most important privacy practices to help users clearly understand the privacy concerns that matter most to them and to make a better informed decision whether to use the product. This evaluation question does not have a "better" or "worse" qualitative component.[65,66,67,68]

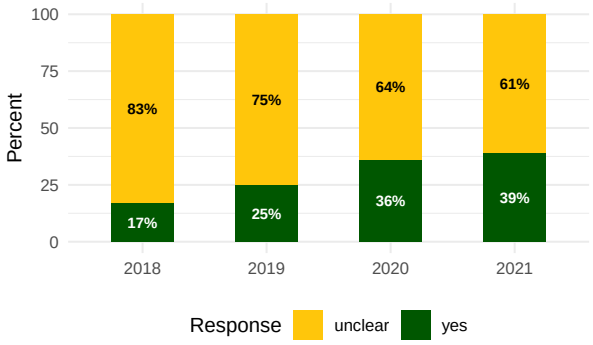
Figure 74: Quick Reference: Do the policies clearly indicate the vendor's privacy principles by short explanations, layered notices, a table of contents, or outlined privacy principles of the vendor?



Preferred Language

The Preferred Language evaluation question indicates whether the policies are available in other languages, or, more importantly, the language most commonly spoken by the user. A company with users in more than one country should provide its policies in all of the languages spoken by its users to ensure adequate notice and informed consent is given by each user to the company's privacy practices. This evaluation question does not have a "better" or "worse" qualitative component.[69]

Figure 75: Preferred Language: Do the policies clearly indicate they are available in any language(s) other than English?



[65] *See* General Data Protection Regulation (GDPR), Subject-matter and objectives, Art. 1(2).

[66] *See* General Data Protection Regulation (GDPR), Subject-matter and objectives, Art. 1(3).

[67] *See* General Data Protection Regulation (GDPR), Principles relating to processing personal data, Art. 5(1)(a).

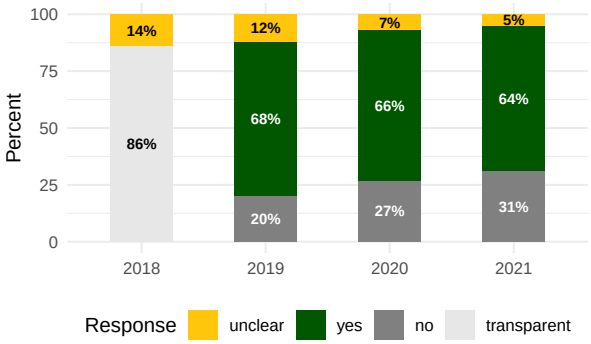
[68] *See* General Data Protection Regulation (GDPR), Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(1).

[69] *See* General Data Protection Regulation (GDPR), Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(1).

Children Intended

The Children Intended evaluation question indicates whether children under 13 years of age are the intended audience of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users, especially children. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.[70,71]

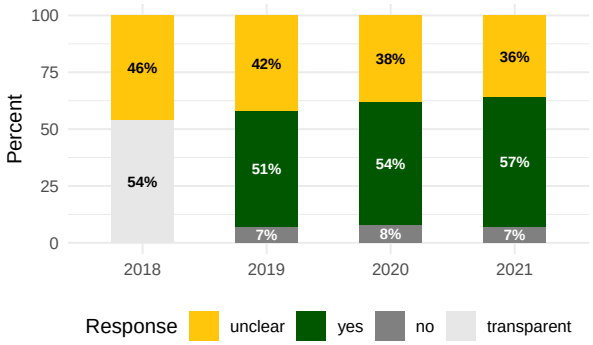
Figure 76: Children Intended: Do the policies clearly indicate whether or not the product is intended to be used by children under the age of 13?



Teens Intended

The Teens Intended evaluation question indicates whether teens over 13 years of age, but under 18 years of age, are the intended audience of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users, including teens under the age of majority in their respective country. This evaluation question does not have a "better" or "worse" qualitative component. [72,73,74]

Figure 77: Teens Intended: Do the policies clearly indicate whether or not the product is intended to be used by teens 13 to 18 years of age?



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

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

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

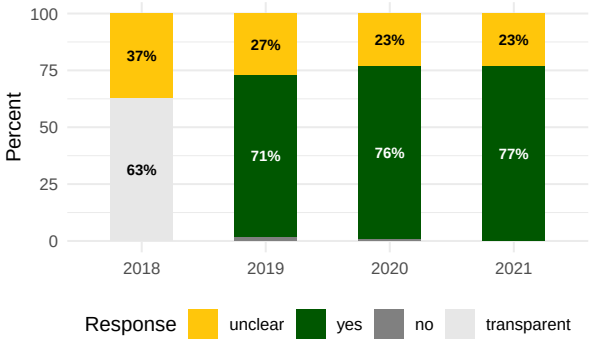
[73] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.

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

Adults Intended

The Adult Intended evaluation question indicates whether individuals over the age of majority in their respective country are the intended audience of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users. This evaluation question does not have a "better" or "worse" qualitative component.[75,76]

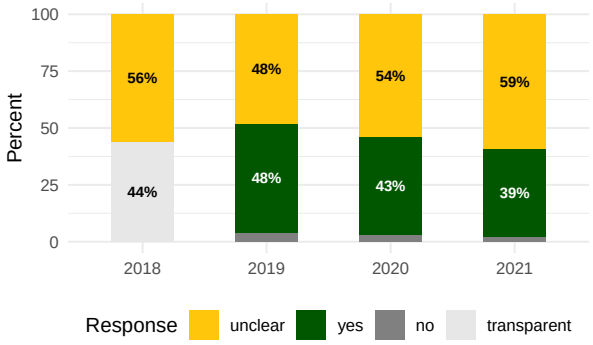
Figure 78: Adults Intended: Do the policies clearly indicate whether or not the product is intended to be used by adults over the age of 18?



Parents Intended

The Parents Intended evaluation question indicates whether individuals with children who are users of the product are also the intended audience of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users which include the ability of parent users to manage child profiles and provide consent on behalf of their children. This evaluation question does not have a "better" or "worse" qualitative component.[77]

Figure 79: Parents Intended: Do the policies clearly indicate whether or not the product is intended to be used by parents or guardians?



[75] *See* General Data Protection Regulation (GDPR), Subject-matter and objectives, Art. 1(1).

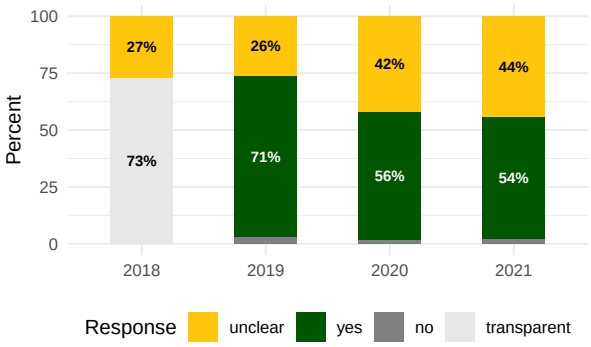
[76] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(i).

[77] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(i)-(iv); *See also* 15 U.S.C. § 6501(9).

Students Intended

The Students Intended evaluation question indicates whether children under 13 years of age and teens over 13 years of age, but under 18 years of age, are the intended audience of the product for use in a K-12 school or district. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users, including students with additional federal and state student data privacy laws. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.[78,79,80,81,82]

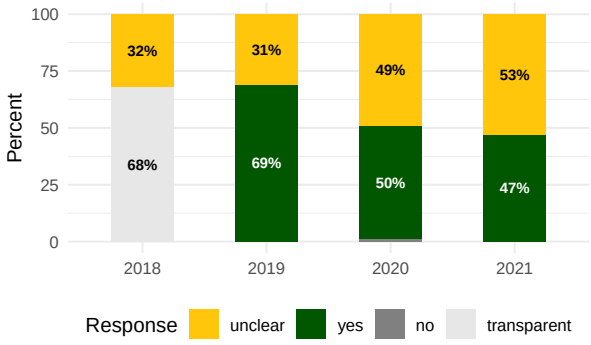
Figure 80: Students Intended: Do the policies clearly indicate whether or not the product is intended to be used by students in preschool or K-12?



Teachers Intended

The Teachers Intended evaluation question indicates whether individuals in a K-12 school or district with students who are users of the product are also the intended audience of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users, which include the ability of teacher users to manage student accounts and provide consent on behalf of their parents. This evaluation question does not have a "better" or "worse" qualitative component.[83,84,85]

Figure 81: Teachers Intended: Do the policies clearly indicate whether or not the product is intended to be used by teachers?



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

[79] *See* Early Learning Personal Information Protection Act (ELPIPA), Cal. B.&P. Code § 22586(a)(1).

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

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

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

[83] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1; *See also* 34 C.F.R. Part 99.30.

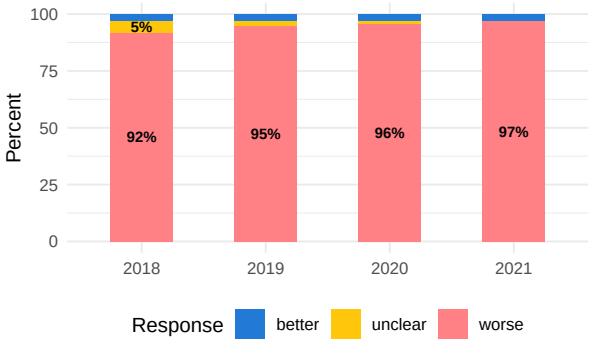
[84] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(a).

[85] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1.

Collect PII

The Collect Personally Identifiable Information evaluation question indicates whether or not personal information is collected by the product and how that personal information is collected. A company should disclose whether the product collects personal information from any user, because the collection of personal information can increase risk depending on the amount of personal information collected and how it is used. A "better" response to this evaluation question indicates the product does not collect personal information. This question is also included in our basic evaluation process.[86,87,88,89,90,91]

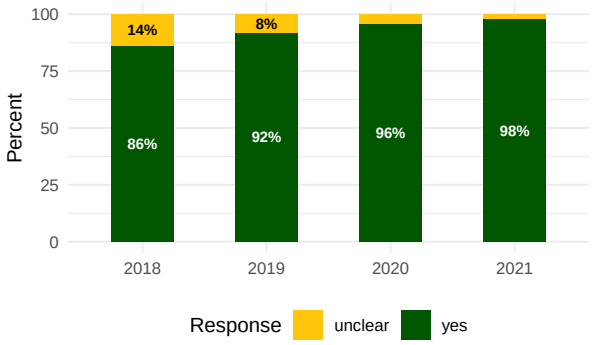
Figure 82: Collect PII: Do the policies clearly indicate whether or not the vendor collects personally identifiable information (PII)?



PII Categories

The Personally Identifiable Information Category evaluation question indicates what categories of personal information are collected by the product. A company should disclose what categories of personal information the product collects from any user, because the collection of personal information can increase risk depending on what types of personal information are collected and how it is used. This evaluation question does not have a "better" or "worse" qualitative component.[92,93,94,95,96,97,98,99]

Figure 83: PII Categories: Do the policies clearly indicate what categories of personally identifiable information are collected by the product?



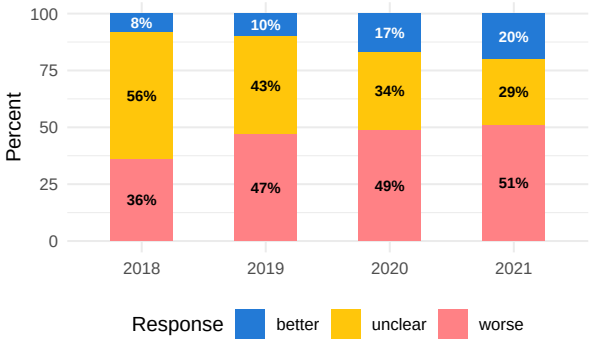
[86] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.6(a)(2).
[87] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1.
[88] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22577(a)(1)-(6).
[89] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.110(a)(5).
[90] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(f), (v)(1).
[91] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(1).

[92] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(1).
[93] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part312.6(a)(1).
[94] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(a)(1).
[95] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.110(a)(1).
[96] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.115(a)(1).
[97] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(5)(B)(i).
[98] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(v)(1)(B), (x).
[99] *See* General Data Protection Regulation (GDPR), Art. 14(1)(d), 15(1)(b).

Geolocation Data

The Geolocation Data evaluation question indicates whether or not precise location information is collected from the product or derived from usage information including GPS, IP address, or other methods. A company should disclose whether precise location information is collected and how that information is collected because there is an increased risk if a user's exact location is known in real time or can be tracked over time. A "better" response to this evaluation question indicates the product does not collect precise location information.[100,101,102,103,104,105]

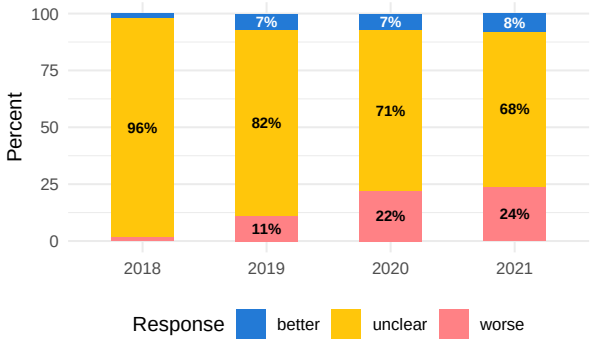
Figure 84: Geolocation Data: Do the policies clearly indicate whether or not precise geolocation data are collected?



Health Data

The Health Data evaluation question indicates whether or not health or biometric data is collected by the product. This may include body movements, heart rate, fingerprint, iris scan, or other biological activity related to a specific individual. A company should disclose whether health or biometric information is collected and how that information is collected, because there is an increased risk if a user's health information is used for unintended purposes. A "better" response to this evaluation question indicates the product does not collect health or biometric data.[106,107,108,109,110]

Figure 85: Health Data: Do the policies clearly indicate whether or not any health or biometric data are collected?



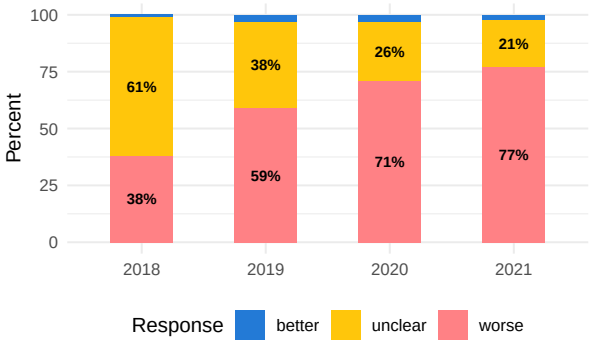
[100] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[101] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.
[102] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).
[103] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22577(a)(1)-(6).
[104] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(w).
[105] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(1).

[106] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.
[107] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[108] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).
[109] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(c).
[110] *See* General Data Protection Regulation (GDPR), Art. 4(1), 4(13), 4(14), 4(15).

Behavioral Data

The Behavioral Data evaluation question indicates whether or not a user's interactions, behaviors, or usage analytics with the product are collected. For example, behavioral data can include which features are used or not used, which buttons or controls are clicked, and which content is viewed, what other users viewed that same content and when, and the duration of interactions with the product and other users – all of which can all be used to create a behavioral profile of the user. The collection of behavioral data can reveal significant information about a user's preferences, habits, and vulnerabilities that can increase risk if used for unintended purposes. A "better" response to this evaluation question indicates the product does not collect a user's interactions, behaviors, or usage analytics.[111,112,113,114]

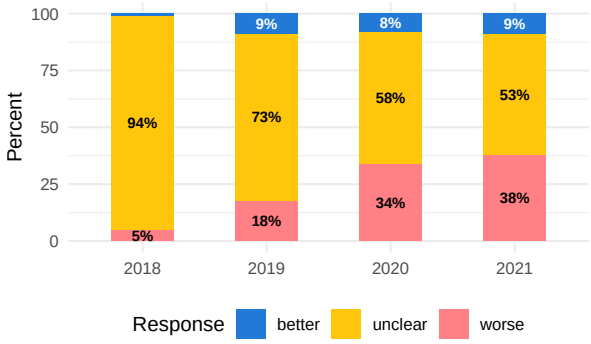
Figure 86: Behavioral Data: Do the policies clearly indicate whether or not any behavioral data are collected?



Sensitive Data

The Sensitive Data evaluation question indicates whether or not specific information protected under federal or state law is collected by the product. For example, sensitive data can include race, ethnicity, gender, sexual identity, religion, political affiliation, national origin, and financial information. The collection of sensitive data can reveal significant information about a user that can increase risk if used for discriminatory or unintended purposes. A "better" response to this evaluation question indicates the product does not collect a user's sensitive data.[115,116,117,118]

Figure 87: Sensitive Data: Do the policies clearly indicate whether or not sensitive personal information is collected?



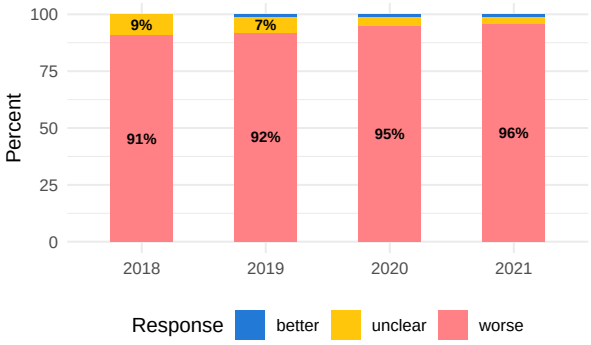
[111] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[112] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.
[113] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(r), (s).
[114] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(14).

[115] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(a)(2).
[116] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.121(a)-(b).
[117] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(v)(1)(L), (ae).
[118] *See* General Data Protection Regulation (GDPR), Processing of special categories of personal data, Art. 9(1)-(2)(a).

Usage Data

The Usage Data evaluation question indicates whether or not a user's device information or technical analytics with the product are collected. For example, usage data can include a user's IP address, device unique identifier, advertising identifier, persistent cookies, time stamps, amount of data downloaded or uploaded, filenames, network IDs, or other identifiers. The collection of usage data can reveal significant information about a user's devices used to access the product and identity that can increase risk if used for unintended purposes. A "better" response to this evaluation question indicates the product does not automatically collect a user's usage data.[119,120,121,122,123,124]

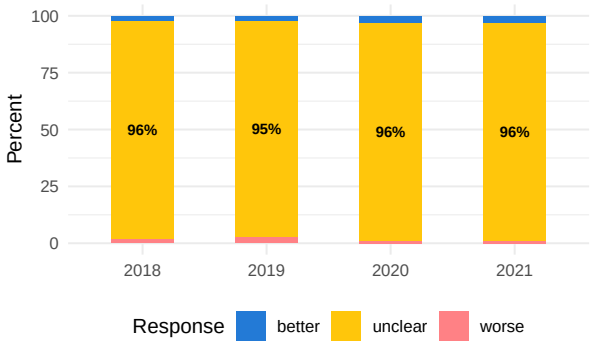
Figure 88: Usage Data: Do the policies clearly indicate whether or not the product automatically collects any information?



Lunch Status

The Lunch Status evaluation question indicates whether or not specific information protected under federal law is collected by the product. A company should disclose whether they collect information from students that is related to free and reduced lunch status because of the increased risk if used for discriminatory or unintended purposes. A "better" response to this evaluation question indicates the product does not collect a student's lunch status information.[125,126]

Figure 89: Lunch Status: Do the policies clearly indicate whether or not the vendor collects information on free or reduced lunch status?



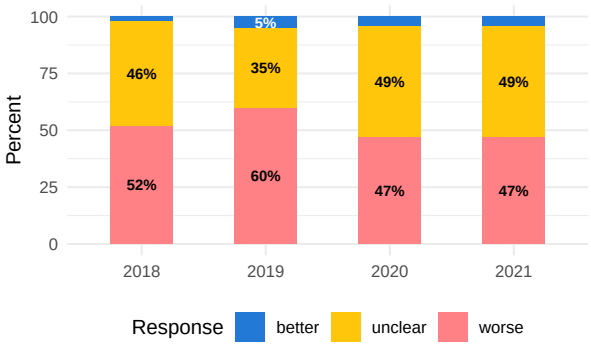
[119] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[120] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.
[121] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).
[122] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22577(a)(1)-(6).
[123] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(v)(1)(F).
[124] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(1).

[125] *See* The National School Lunch Act (NSLA), 42 U.S.C. §§ 1751-63.
[126] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

Student Data

The Student Data evaluation question indicates whether information related to a student's use of the product in a K-12 school or district is collected for education purposes. A company should disclose whether student data is collected from any user of the product because of the additional student data privacy protections required for collection and use of education records under federal and state law. A "better" response to this evaluation question indicates the product does not collect student data.[127,128]

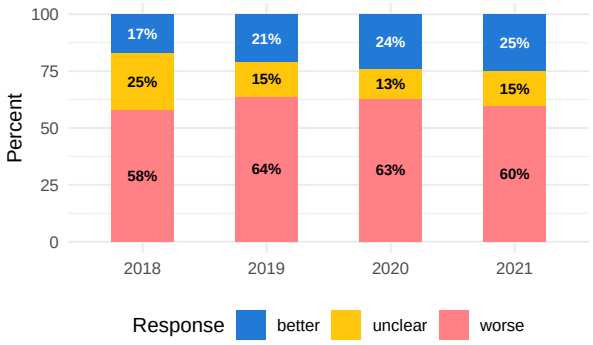
Figure 90: Student Data: Do the policies clearly indicate whether or not the vendor collects personal information or education records from preK-12 students?



Child Data

The Child Data evaluation question indicates whether information related to a child under 13 years of age is collected by the product. A company should disclose whether child data is collected from any user of the product because of the additional privacy protections required for the collection and use of children's personal information under federal law. A "better" response to this evaluation question indicates the product does not collect child data.[129]

Figure 91: Child Data: Do the policies clearly indicate whether or not the vendor collects personal information online from children under 13 years of age?



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

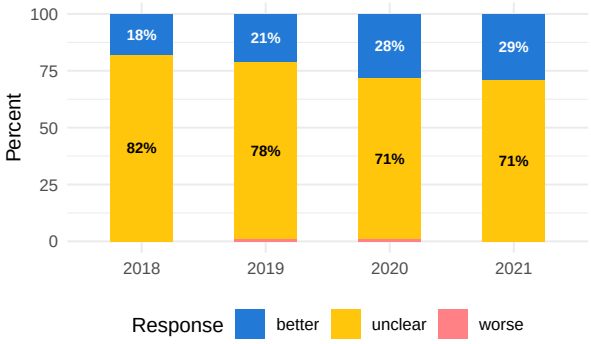
[128] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(a); *See also* § 22586(a)(1).

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

Data Excluded

The Data Excluded evaluation question indicates whether specific types of personal information are excluded from collection by the product either because of a concern for the sensitive nature of the information, or that a third-party service provider may collect that type of personal information on behalf of the company. A company should minimize the collection of information to only data required to provide the product and exclude collection of unnecessary data. A "better" response to this evaluation question indicates that specific types of personal information are excluded from collection by the product due to its nature.

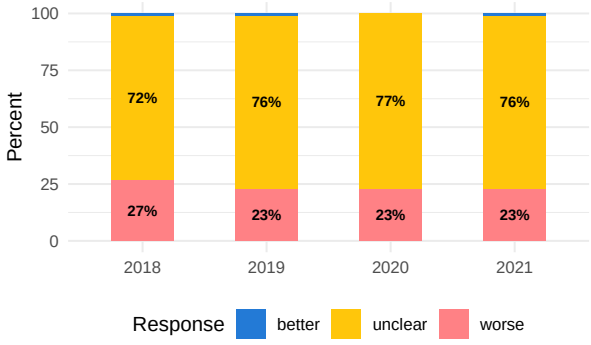
Figure 92: Data Excluded: Do the policies clearly indicate whether or not the vendor excludes specific types of data from collection?



Coverage Excluded

The Coverage Excluded evaluation question indicates whether specific types of personal information that are collected by the product or third parties are excluded from the scope of the privacy policy either because of a concern for the sensitive nature of the information, or that a third-party service provider's policies cover the data collection and use practices for that type of personal information. A company should not collect personal information from users that is not covered by the product's privacy policies to ensure users have adequate notice of how their data will be collected and used in order to provide informed consent. A "better" response to this evaluation question indicates the product does exclude collected information from the company's privacy policy.

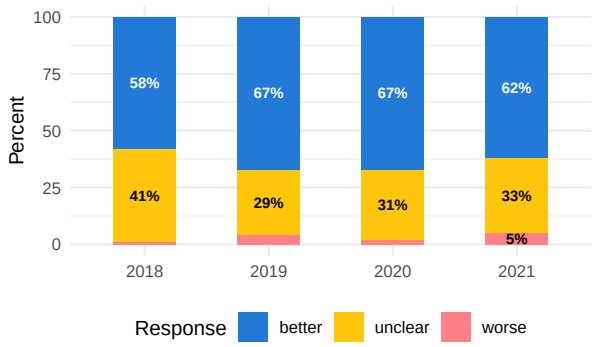
Figure 93: Coverage Excluded: Do the policies clearly indicate whether or not the vendor excludes specific types of collected data from coverage under its privacy policy?



Collection Limitation

The Collection Limitation evaluation question indicates whether personal information is only collected that is necessary for providing the primary purpose of the product. A company should practice data minimization principles and only collect the minimum amount of data required to provide the product to users in order to decrease the risk that a user's data is used for unintended purposes. A "better" response to this evaluation question indicates the product does limit its collection of personal information. This question is also included in our basic evaluation process.[130,131,132]

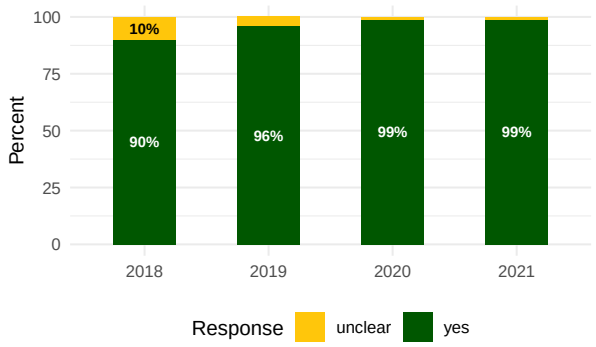
Figure 94: Collection Limitation: Do the policies clearly indicate whether or not the vendor limits the collection or use of information to only data that are specifically required for the product?



Data Shared

The Data Shared evaluation question indicates whether the product shares a user's data with third parties in order to provide the service. Sharing a user's data with third parties is not qualitatively better or worse because it is often a necessary requirement to provide all the features of a product that includes sharing data with third-party service providers such as SDKs, cloud hosting, content integrations, or payment processors. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.[133,134,135,136,137]

Figure 95: Data Shared: Do the policies clearly indicate if collected information (this includes data collected via automated tracking or usage analytics) is shared with third parties?



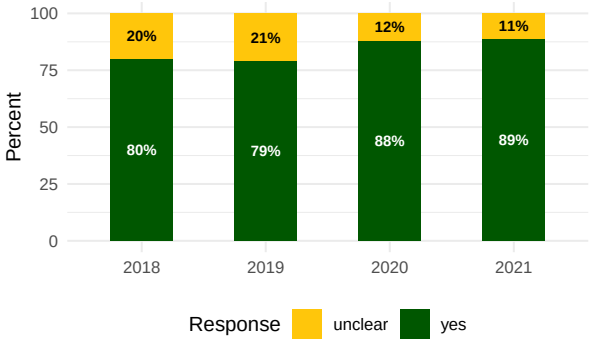
[130] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.7.
[131] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(c).
[132] *See* General Data Protection Regulation (GDPR), Art. 5(1)(c), 7(4), 25(1).

[133] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.8.
[134] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.
[135] *SeE* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(4), 22584(b)(4)(B)-(C),(k).
[136] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ah).
[137] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(10).

Data Categories

The Data Categories evaluation question indicates whether the product shares a user's data with third parties and what type or categories of data are shared in order to provide the service. Disclosing the categories of personal information that is shared with third parties is not qualitatively better or worse because it is often a necessary requirement to share data to provide all the features of a product that includes sharing data with third-party service providers. A company should disclose what types of personal data are shared with third parties to ensure users have adequate notice if only some types or all of their data will be shared with third parties in order to provide informed consent. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.[138,139,140]

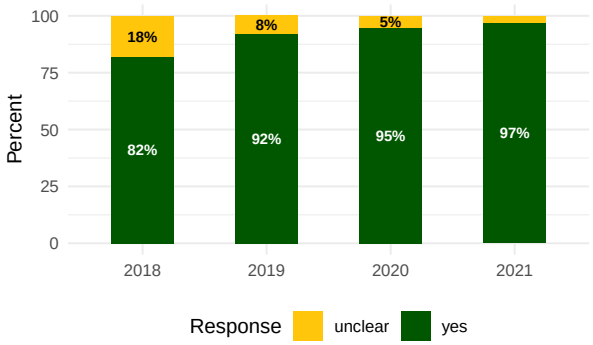
Figure 96: Data Categories: Do the policies clearly indicate what categories of information are shared with third parties?



Sharing Purpose

The Sharing Purpose evaluation question indicates why a user's data is shared with third parties. A company should disclose the reasons why personal data is shared with third parties because it provides users with notice of how their data could be used by other companies, which could increase risk if used for unintended purposes. This evaluation question does not have a "better" or "worse" qualitative component.[141,142,143,144]

Figure 97: Sharing Purpose: Do the policies clearly indicate the vendor's intention or purpose for sharing a user's personal information with third parties?



[138] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.115(c)(2).

[139] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part312.6(a)(1).

[140] *See* General Data Protection Regulation (GDPR), Art. 14(1)(d), 15(1)(b).

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

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

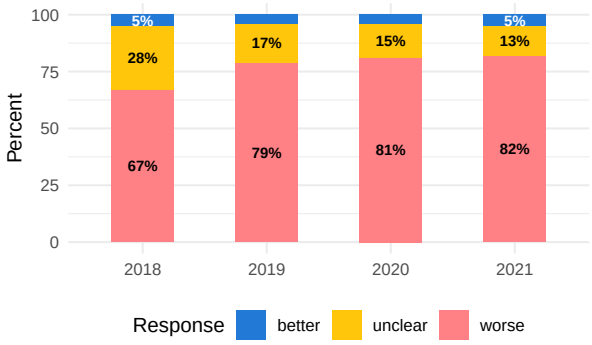
[143] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e).

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

Third-Party Analytics

The Third-Party Analytics evaluation question indicates whether the product automatically collects usage data from a user based on their use of the product and then shares that data with a third-party analytics provider to better understand how their service is used. A company should disclose the name of any third-party analytics services that receive a user's data and take steps to minimize the amount of data sent to third parties for analytics purposes, which could increase risk if used for unintended purposes. A "better" response to this evaluation question indicates the product does not disclose a user's data to a third-party analytics provider.[145,146,147,148]

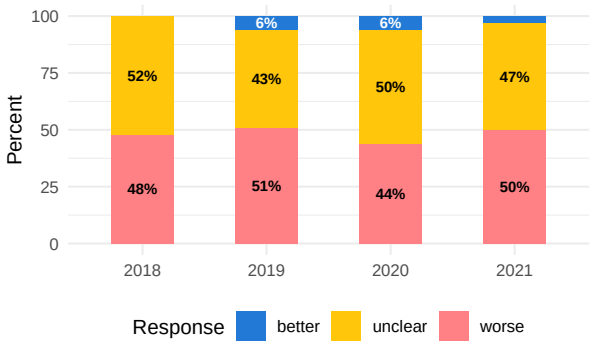
Figure 98: Third-Party Analytics: Do the policies clearly indicate whether or not collected information is shared with third parties for analytics and tracking purposes?



Third-Party Research

The Third-Party Research question indicates whether personal and behavioral data from users' use of the product is disclosed to third parties for their own research purposes. A company should disclose what types of personal data are used for testing or research purposes because this practice is not the primary purpose of providing the product to users, and the risk of third parties re-identifying previously de-identified or anonymized data could be used for unintended purposes. However, companies can mitigate these risks by de-identifying or anonymizing children's and students' 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. A "better" response to this evaluation question indicates the product does not disclose a user's data to third parties for their own research purposes.[149,150,151,152,153,154]

Figure 99: Third-Party Research: Do the policies clearly indicate whether or not collected information is shared with third parties for research or product improvement purposes?



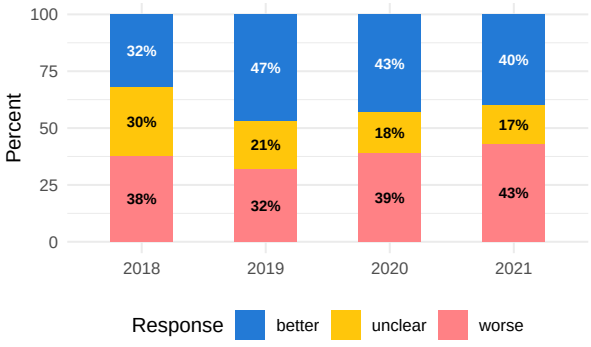
[145] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[146] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(1)(A), 22584(b)(2).
[147] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(5).
[148] *See* General Data Protection Regulation (GDPR), Processing of special categories of personal data, Art. 9(1)-(2)(j).

[149] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[150] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.31(a)(6), 99.31(b)(2).
[151] *See* Protection of Pupil Rights Act (PPRA), 34 C.F.R. § 98.3.
[152] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(e)(2), 22584(b)(4), 22584(l).
[153] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49074.
[154] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ab).

Third-Party Marketing

The Third-Party Marketing evaluation question indicates whether marketing communications that could include emails, text messages, or other notifications are sent to users are from an application or service that a user does not have a direct relationship with and therefore has different expectations, because it communicates unrelated or unsolicited products and features from third-party companies. A "better" response to this evaluation question indicates the product does not send third-party marketing communications to users. This question is also included in our basic evaluation process.[155,156,157,158,159,160]

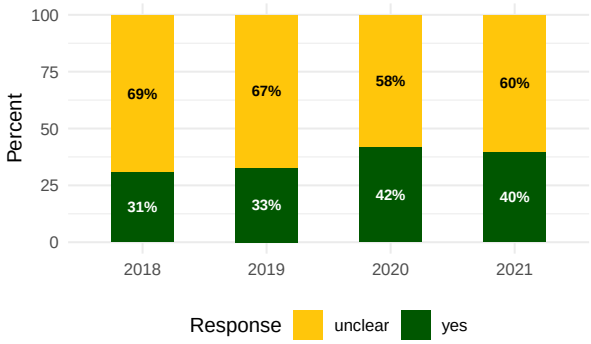
Figure 100: Third-Party Marketing: Do the policies clearly indicate whether or not personal information is shared with third parties for advertising or marketing purposes?



Exclude Sharing

The Exclude Sharing evaluation question indicates whether specific types of personal information or information from a particular type of user that are collected by the product are excluded from sharing with third parties, because of a concern for the sensitive nature of the information. A company should not share personal information from users with third parties if disclosure is not required to provide the service. This best practice ensures users have better protection of their most sensitive personal information because it minimizes disclosure to third parties that could use the data for unintended purposes. This evaluation question does not have a "better" or "worse" qualitative component.

Figure 101: Exclude Sharing: Do the policies specify any categories of information that will not be shared with third parties?

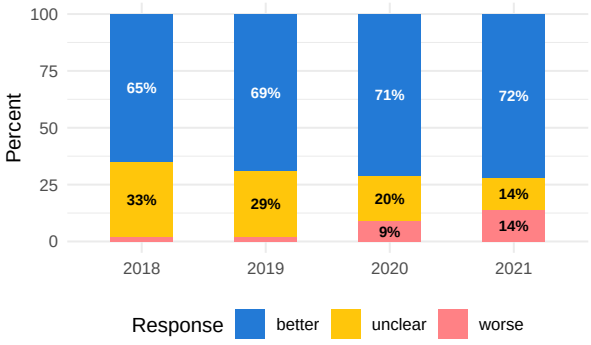


[155] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[156] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).
[157] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.
[158] *See* Shine The Light, Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.
[159] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(a).
[160] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(6).

Sell Data

The Sell Data evaluation question indicates whether the policies disclose a user's personal information is sold or rented to third parties for monetary or other valuable consideration. Selling users' data is an important issue for a policy to disclose because users want to know if their data is shared with third parties in exchange for use of the product, which may impact their decision whether to use the product or service. A "better" response to this evaluation question indicates the product does not sell a user's data to third parties. This question is also included in our basic evaluation process.[161,162,163,164,165,166]

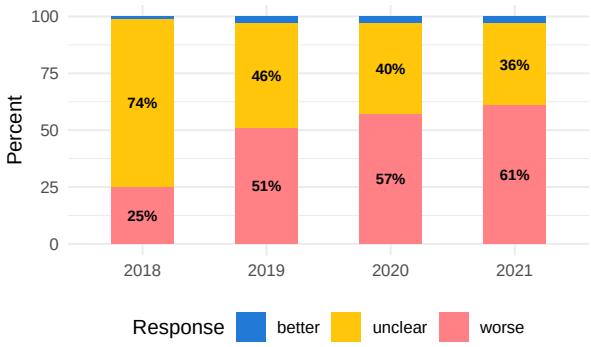
Figure 102: Sell Data: Do the policies clearly indicate whether or not a user's personal information is sold or rented to third parties?



Data Acquired

The Data Acquired evaluation question indicates whether personal information is purchased or acquired by the company from third-party companies such as data brokers to augment or supplement the data the company already collects from individual users to further personalize the service. A company should disclose whether data about a user is acquired from other sources than the product because it increases risk that a user's data may be used for unintended purposes. A "better" response to this evaluation question indicates the product does not purchase data about users from third parties.[167,168,169,170,171,172,173]

Figure 103: Data Acquired: Do the policies clearly indicate whether or not the vendor may acquire a user's information from a third party?



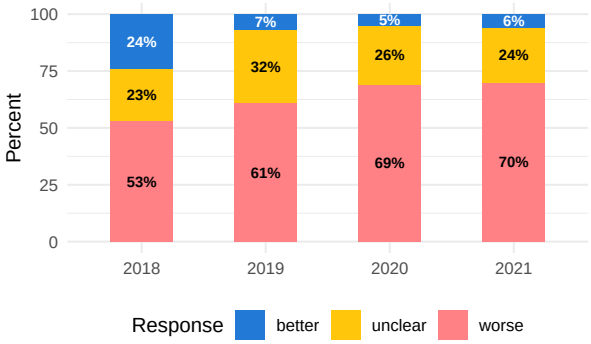
[161] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[162] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).
[163] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.120(b)-(c).
[164] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.135(a).
[165] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ad)(1).
[166] *See* General Data Protection Regulation (GDPR), Art. 13(2)(b), 14(2)(c), 15(1)(e), 18(1)(d), 21(1), 21(4).

[167] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(1).
[168] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22577(a)(1)-(6).
[169] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.110(a)(2).
[170] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(5)(B)(i).
[171] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(v)(2).
[172] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(f).
[173] *See* General Data Protection Regulation (GDPR), Right of access by the data subject, Art. 15(1)(g).

Outbound Links

The Outbound Links evaluation question indicates whether notice is provided to the user if they interact with hyperlinks, buttons, or other actions that cause the user to leave the product to access third-party content or resources that may not be age-appropriate. A company should notify users about any actions taken that cause them to leave the product and potentially subject themselves to different third-party privacy practices or age-inappropriate content. A "better" response to this evaluation question indicates the product does notify users that they are leaving the product.[174]

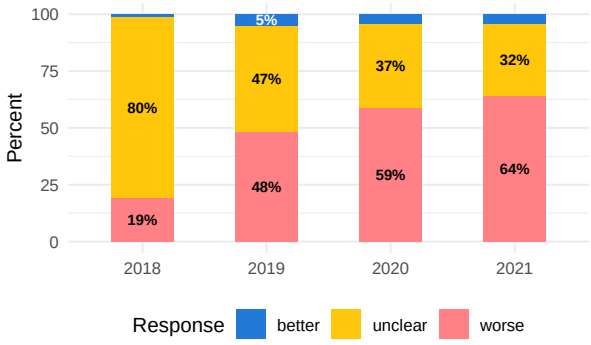
Figure 104: Outbound Links: Do the policies clearly indicate whether or not outbound links on the site to third-party external websites are age-appropriate?



Authorized Access

The Authorized Access evaluation question indicates whether the product allows the integration of third-party services to access a user's personal information collected by the product to provide additional features. A company should disclose the names of any third-party services that may access a user's information because it increases the risk that a user's data may be used for unintended purposes. A "better" response to this evaluation question indicates the product does not provide third parties with authorization to access a user's data any time.[175]

Figure 105: Authorized Access: Do the policies clearly indicate whether or not a third party is authorized to access a user's information?



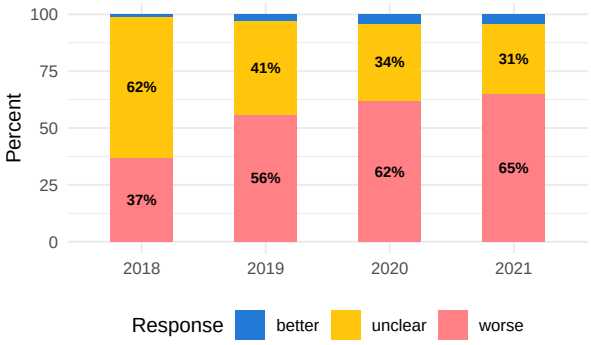
[174] *See* Children's Internet Protection Act (CIPA), 47 U.S.C. § 254.

[175] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(1).

Third-Party Collection

The Third-Party Collection evaluation question indicates whether the product allows the integration of third-party services to collect a user's personal information when using the product to provide additional features. A company should disclose the names of any third-party services that may collect a user's information because it increases the risk that a user's data may be used for unintended purposes. A "better" response to this evaluation question indicates the product does not allow authorized third parties to collect personal information of users any time through the product. [176]

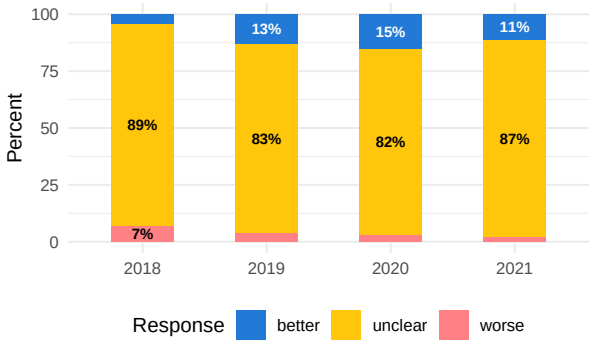
Figure 106: Third-Party Collection: Do the policies clearly indicate whether or not a user's personal information is collected by a third party?



Data Misuse

The Data Misuse evaluation question indicates whether a user's personal information may be deleted or restricted from a third-party service provider if the third party's use of data is in breach of the company's agreement with the third-party company or the company's privacy policies. A company should protect any of their users' data that is shared with a third party by preventing any third-party misuse of data for unintended purposes. A "better" response to this evaluation question indicates the product does provide a process to delete or restrict a user's data from a third party if misused. [177,178,179]

Figure 107: Data Misuse: Do the policies clearly indicate whether or not a user's information can be deleted from a third party by the vendor, if found to be misused by the third party?



[176] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(6).

[177] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(d)(5).

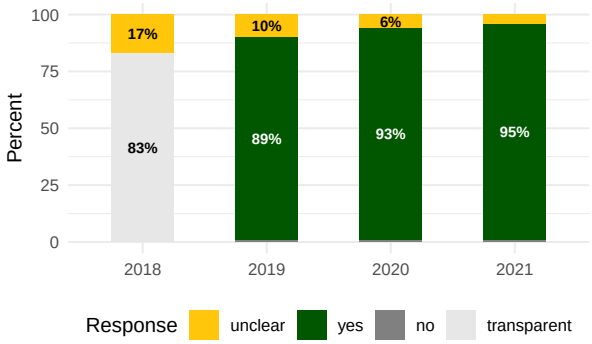
[178] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(j)(1)(C).

[179] *See* General Data Protection Regulation (GDPR), Processor, Art. 28(3).

Third-Party Providers

The Third-Party Provider evaluation question indicates whether the product shares a user's data with third-party service providers as a requirement to provide the service. It is important that companies 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. This evaluation question does not have a "better" or "worse" qualitative component.[180,181,182,183,184,185]

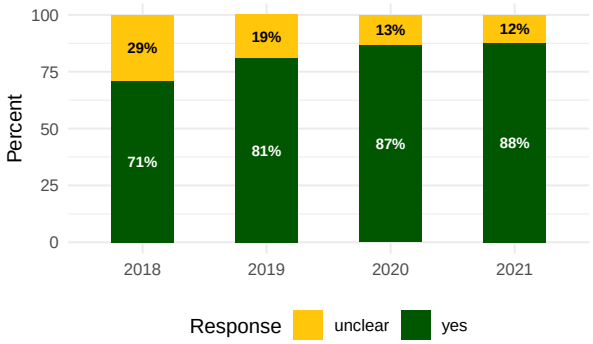
Figure 108: Third-Party Providers: Do the policies clearly indicate whether or not third-party services are used to support the internal operations of the vendor's product?



Third-Party Roles

The Third-Party Roles evaluation question indicates the purpose of a third-party service provider that the product shares users' data. It is important for a company to clearly explain and define the role third parties have in supporting the internal operations of the company'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 reason the company is 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. This evaluation question does not have a "better" or "worse" qualitative component.[186,187,188,189]

Figure 109: Third-Party Roles: Do the policies clearly indicate the role of third-party service providers?



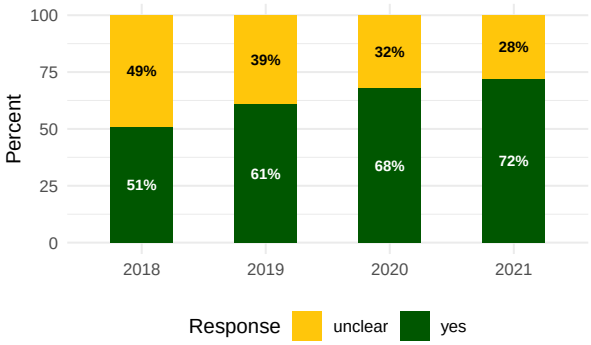
[180] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[181] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(i).
[182] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(1).
[183] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(3)(A).
[184] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(j)(1), (e)(5), (ag)(1).
[185] *See* General Data Protection Regulation (GDPR), Art. 13(1)(e), 14(1)(e), 15(1), 28(3).

[186] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[187] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(i).
[188] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(1).
[189] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(5).

Third-Party Categories

The Third-Party Categories evaluation question indicates the types and names of third-party companies such as affiliates, subsidiaries, or partners that a product shares a user's data with for purposes unrelated to providing the service. It is important for a company to clearly explain and define the role of third parties that have access to users' data but provide no support for the internal operations of the company's product. It is not sufficient to state that a user's data is shared with a related third party without also clarifying how that third party uses the shared information. Clarifying the role of related third parties helps parents and educators make a more informed decision by better understanding the purpose of the company sharing data with different categories of third parties. This evaluation question does not have a "better" or "worse" qualitative component.[190,191,192,193,194]

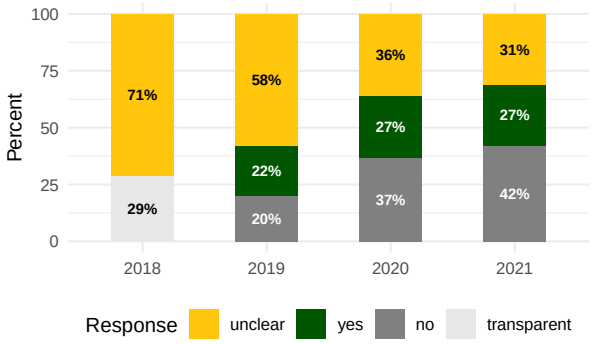
Figure 110: Third-Party Categories: Do the policies clearly indicate the categories of related third parties, such as subsidiaries or affiliates with whom the vendor shares data?



Third-Party Policy

The Third-Party Policy evaluation question indicates whether notice is provided of any privacy policy links or URLs for any third-party service providers or third-party companies that may access a user's personal information. A company should disclose links to the privacy policies of any third-party company that the product may share a user's personal information with so users can make a more informed decision by better understanding the privacy practices of the third parties who may access their data. This evaluation question does not have a "better" or "worse" qualitative component.

Figure 111: Third-Party Policy: Do the policies clearly indicate whether or not the vendor provides a link to a third-party service provider, data processor, partner, or affiliate's privacy policy?

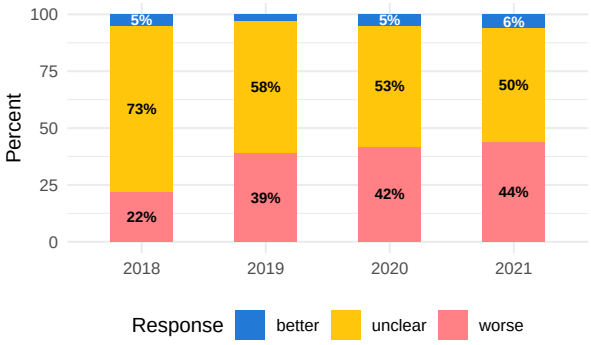


[190] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(1).
[191] *See* General Data Protection Regulation (GDPR), Art. 13(1)(e), 14(1)(e).
[192] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.110(a)(4).
[193] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(d)(2)-(3).
[194] *See* General Data Protection Regulation (GDPR), Right of access by the data subject, Art. 15(1)

Vendor Combination

The Vendor Combination evaluation question indicates whether information collected from the product is combined with other information acquired by the company from third-party sources. A company should disclose whether a user's data is augmented or supplemented for purposes unrelated to proving the service because the risk could increase if the combined data is used by the company or third parties for unintended purposes. A "better" response to this evaluation question indicates the product does not combine a user's data with other third-party sources.[195]

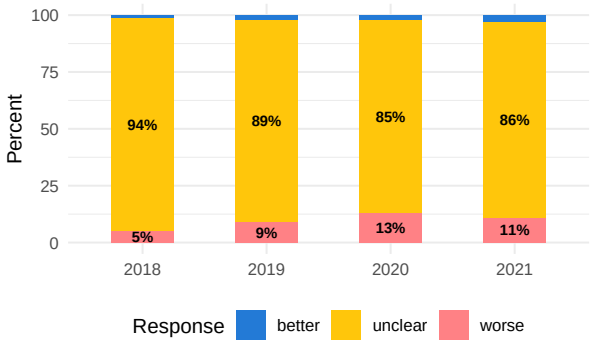
Figure 112: Vendor Combination: Do the policies clearly indicate whether or not data collected or maintained by the vendor can be augmented, extended, or combined with data from third-party sources?



Third-Party Combination

The Third-Party Combination evaluation question indicates whether third parties may combine a user's information shared with them by a first-party company that has a direct relationship with their user with other information acquired from other third-party sources for their own purposes. A company should place contractual restrictions on third-party companies that receive users' personal information from the product because of the increased risk the combined data is used for unintended purposes. A "better" response to this evaluation question indicates third parties may not combine a user's information from the product with their own third-party sources of information.[196,197]

Figure 113: Third-Party Combination: Do the policies clearly indicate whether or not data shared with third parties can be augmented, extended, or combined with data from additional third-party sources?



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

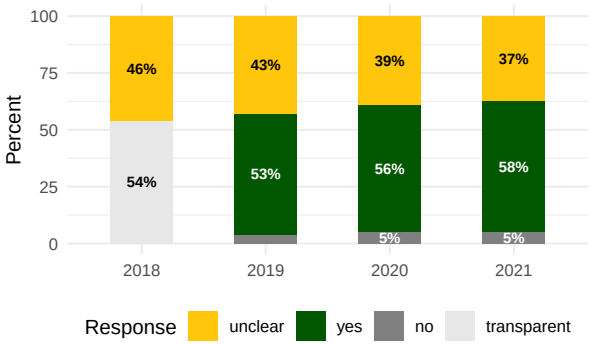
[196] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(i).

[197] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(6).

Social Login

The Social Login evaluation question indicates whether the product incorporates a third-party service provider's federated or social login feature to authenticate users with the product. It is becoming increasingly difficult for consumers, parents, and educators to manage the proliferation of all the applications and services they use themselves, and which are used by their children and students on a daily basis, both at home and in the classroom. Users often see social or federated login features as a quick and convenient alternative to access a product instead of managing countless user account names and passwords. In order to streamline the account-creation process, outsource account management, and outsource authorization practices, many companies have incorporated social or federated login options into their products. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.[198]

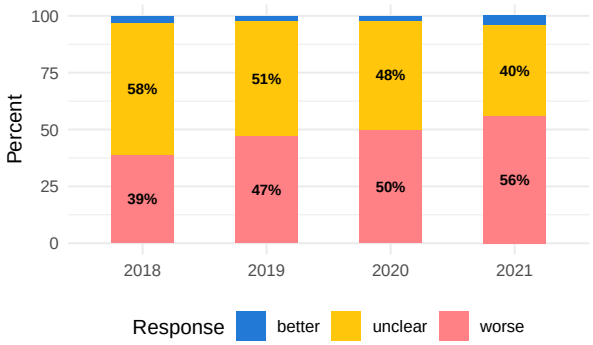
Figure 114: Social Login: Do the policies clearly indicate whether or not social or federated login is supported to use the product?



Social Collection

The Social Collection evaluation question indicates whether the product collects personal information from the integration of third-party social networking features or social login account that could be used to augment or supplement a user's personal information collected by the product. A "better" response to this evaluation question indicates the product does not collect social login personal information from users.[199]

Figure 115: Social Collection: Do the policies clearly indicate whether or not the vendor collects information from social or federated login providers?



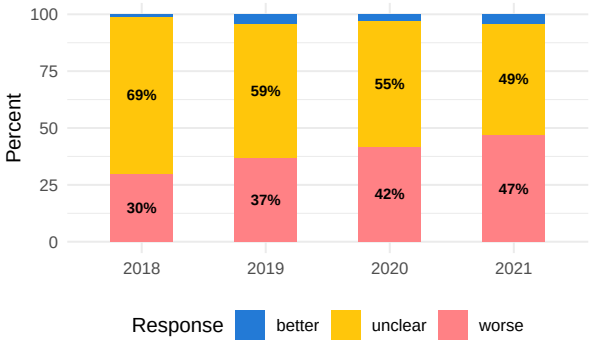
[198] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.6.

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

Social Sharing

The Social Sharing evaluation question indicates whether the product may disclose personal information collected from the product with a third-party social networking service. A company should disclose whether data about a user can be shared publicly on third-party social media because it increases risk that a user's data may be used for unintended purposes. A "better" response to this evaluation question indicates the product does not disclose personal information from users to others on a social networking service.

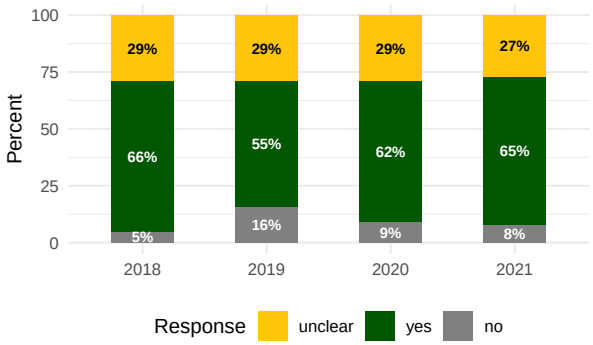
Figure 116: Social Sharing: Do the policies clearly indicate whether or not the vendor shares information with social or federated login providers?



Data De-identified

The Data De-identified evaluation question indicates whether a user's personal information is disclosed with third parties for their own purposes if the data is de-identified or anonymized by the company before it is shared. Disclosing collected information in an anonymous or de-identified format is a complicated issue and even data that has gone through this process can often be recombined with other data to allow re-identification with only a few known data points. As such, sharing of any information, even information about a user that has been de-identified or anonymized, is a privacy risk. This evaluation question does not have a "better" or "worse" qualitative component.[200,201,202,203,204,205,206]

Figure 117: Data De-identified: 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?

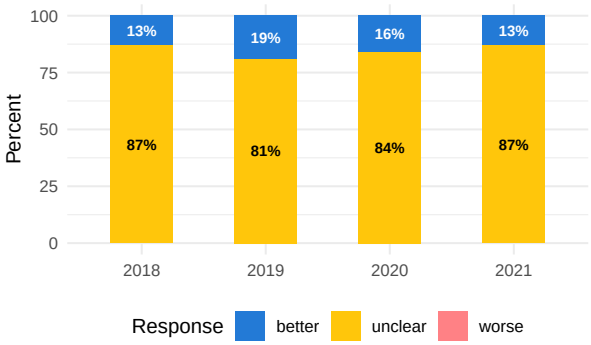


[200] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[201] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.31(b)(1).
[202] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(f)-(g).
[203] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49074.
[204] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(b), (m), (aa).
[205] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.145(a)(6).
[206] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(5), 25(1).

De-identified Process

The De-identified Process evaluation question indicates whether a company provides notice of its de-identification or anonymization process of user data with a reasonable level of justified confidence that data cannot be re-identified by third parties. Companies should disclose that their de-identification 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. 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. A "better" response to this evaluation question indicates the product provides notice of its de-identification or anonymization process.[207,208]

Figure 118: De-identified Process: Do the policies clearly indicate whether or not the deidentification process is done with a reasonable level of justified confidence, or whether the vendor provides links to any information that describes their deidentification process?



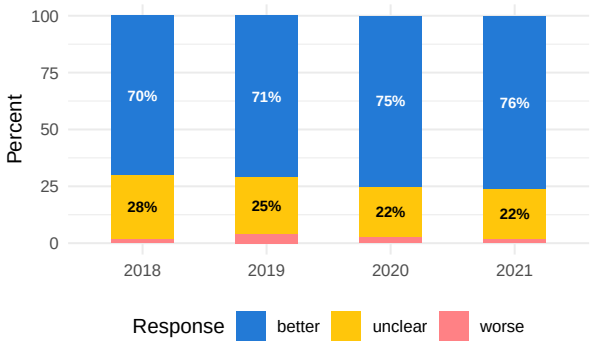
[207] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(b), (m)(A).

[208] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(5).

Third-Party Limits

The Third-Party Limits evaluation question indicates whether the company has placed contractual obligations on any third-party companies that receive a user's data from the product. A company should put in place contractual obligations that require third parties to only collect and use that data in accordance with the company's privacy policy. Without contractual limits on third-party use of data from children and students, parents and educators cannot reasonably expect that the privacy practices outlined in the product's policies will be honored by third parties that have access to personal data. A "better" response to this evaluation question indicates the product does place contractual obligations on third-party companies. This question is also included in our basic evaluation process.[209,210,211,212,213,214,215,216,217]

Figure 119: Third-Party Limits: 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?



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

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

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

[212] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(d)(1)-(4).

[213] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.115(d).

[214] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.121(c).

[215] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.135(f).

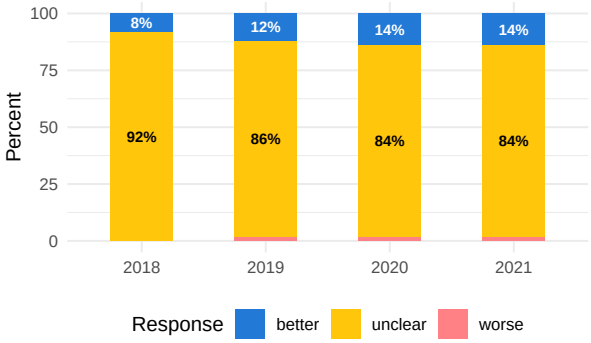
[216] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(j)(1)(A), (j)(2), (m)(B)-(C).

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

Combination Limits

The Combination Limits evaluation question indicates whether the company has placed contractual prohibitions or restrictions on any third-party companies that receive a user's data from the product for re-identification of anonymized or de-identified data. A company should put in place contractual prohibitions that require third parties to not attempt to combine, augment or supplement acquired third-party data about a user with a user's first-party data that has been shared with them by the company, or attempt re-identification of any users in anonymized or de-identified data. A "better" response to this evaluation question indicates the product does place re-identification contractual prohibitions on third-party companies.[218,219,220]

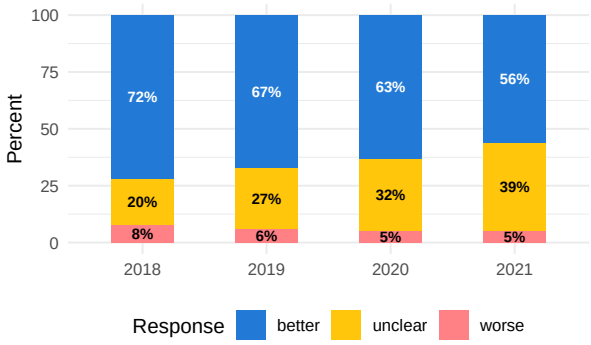
Figure 120: Combination Limits: Do the policies clearly indicate whether or not the vendor imposes contractual limits that prohibit third parties from reidentifying or combining data with other data sources that the vendor shares or sells to them?



Purpose Limitation

The Purpose Limitation evaluation question indicates whether the company limits the use of data collected by the product to only the purpose for which it was collected to provide the service. The purpose of collection can vary between the type of product and type of user if a product's purpose is for educational, entertainment, or content delivery purposes. A company should disclose the purpose for which personal data is collected by the product because there is an increased risk if the data is used for unintended purposes not related to providing the services. A "better" response to this evaluation question indicates the company limits the use of data collected by the product to only the purpose for which it was collected.[221,222,223,224,225]

Figure 121: Purpose Limitation: 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?



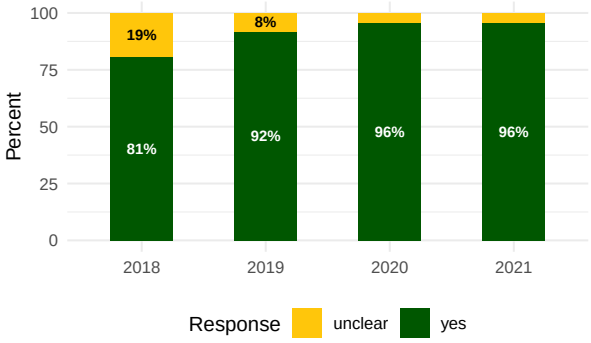
[218] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.8.
[219] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.121(d).
[220] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(j)(1)(A)(i)-(iv).

[221] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10, *See also* 16 C.F.R. Part 312.4(b).
[222] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(3).
[223] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(c).
[224] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(e).
[225] *See* General Data Protection Regulation (GDPR), Principles relating to processing personal data, Art. 5(1)(b), 25(2).

Data Purpose

The Data Purpose evaluation question indicates why a user's personal information is collected by the product and the purpose for which it will be used to provide the service. A company should disclose the reasons it collects different types of data in order to help parents and educators make a more informed decision whether to use the product by better understanding the purpose for which their data is collected and used. This evaluation question does not have a "better" or "worse" qualitative component.[226,227,228,229,230,231]

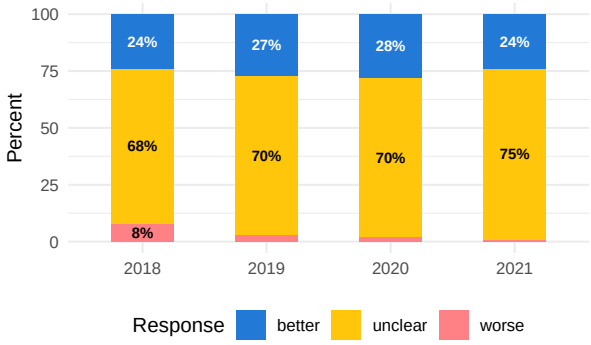
Figure 122: Data Purpose: Do the policies clearly indicate the context or purpose for which data are collected?



Combination Type

The Combination Type evaluation question indicates the type of information data becomes if it is combined with personally identifiable information (PII), which is given special protections. A company should be aware of the risks of combining personally identifiable information (PII) collected by the product with automatically collected non-personally identifiable information or acquired data from third parties. If a user's personal information is combined with any other type of data, the augmented or supplemented data should be treated as PII because of the additional protections given to this data type under federal and state privacy laws. A "better" response to this evaluation question indicates combined information becomes personally identifiable information (PII).[232]

Figure 123: Combination Type: Do the policies clearly indicate whether or not the vendor would treat personally identifiable information (PII) combined with non-personally identifiable information as PII?



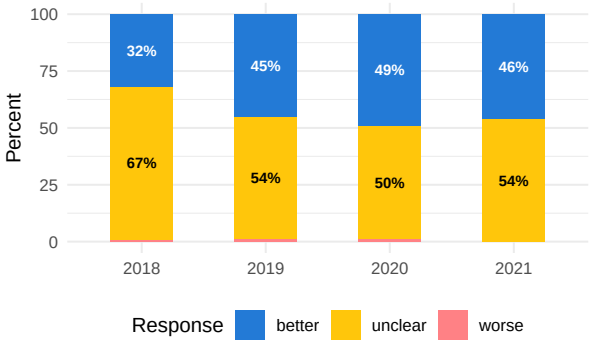
[226] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(b).
[227] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(a)(3).
[228] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.115(c)(2).
[229] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e).
[230] *See* General Data Protection Regulation (GDPR), Art. 13(1)(c), 14(1)(c).
[231] *See* General Data Protection Regulation (GDPR), Right of access by the data subject, Art. 15(1)(a)

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

Context Notice

The Context Notice evaluation question indicates whether notice is given to users if the context or purpose for which their data is collected or used changes from a user's reasonable expectation. A company that intends to process a user's personal information for a different purpose than the data was originally collected should provide the user with notice of the change in context for the other purpose. A "better" response to this evaluation question indicates the user is provided notice if the purpose for which their data is collected or used changes.[233,234,235,236]

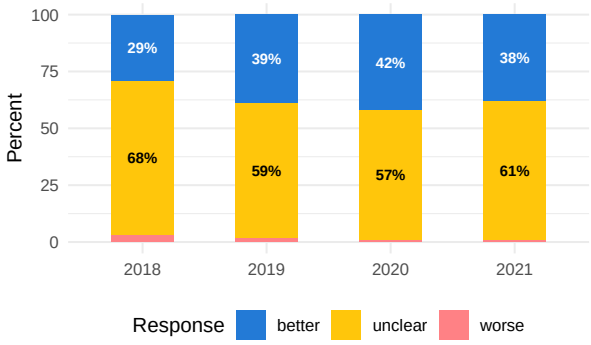
Figure 124: Context Notice: Do the policies clearly indicate whether or not notice is provided to a user if the vendor changes the context in which data are collected?



Context Consent

The Context Consent evaluation question indicates whether informed consent is obtained from a user if the context or purpose in which their data is collected or used changes from the user's reasonable expectation. A company that intends to process a user's personal information for a different purpose than the data was originally collected should obtain consent for the change in context for the other purpose. A "better" response to this evaluation question indicates consent is obtained from the user if the purpose for which their data is collected or used changes.[237]

Figure 125: Context Consent: Do the policies clearly indicate whether or not the vendor will obtain consent if the practices in which data are collected change or are inconsistent with contractual requirements?



[233] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(a)(1)-(2), (c).

[234] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e).

[235] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art. 13(3).

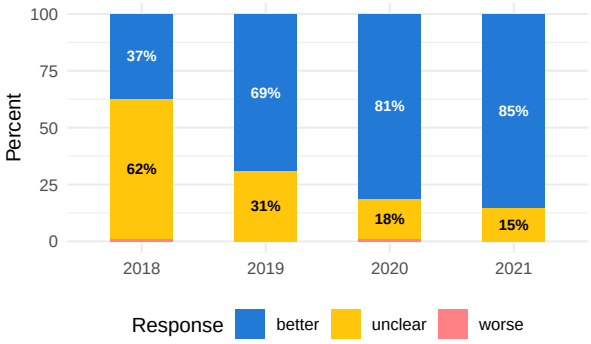
[236] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, GDPR Art. 14(4).

[237] *See* General Data Protection Regulation (GDPR), Lawfulness of Processing, Art. 6(4)(a)-(d).

Community Guidelines

The Community Guidelines evaluation question indicates what type of user content or activities are prohibited on the product and clear examples to help the user understand what the rules are and how they are enforced. A company should disclose that violations of the rules may result in the restriction or termination of a user's account so all users have adequate notice of the product's rules and consequences to help provide a safer environment. A "better" response to this evaluation question indicates the type of user content or activities that are prohibited on the product.

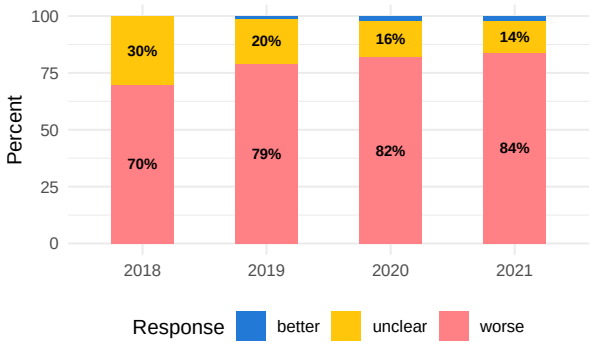
Figure 126: Community Guidelines: Do the policies clearly indicate whether or not the vendor may terminate a user's account if they engage in any prohibited activities?



User Submission

The User Submission evaluation question indicates whether the user may create content or upload user-generated content to the product. User-generated content often contains personal, private, or sensitive information in text, audio, images, photographs, or video format that if inadvertently disclosed to third parties for unintended purposes could cause serious privacy risks and harms. A "better" response to this evaluation question indicates the product does not allow users to create or upload user-generated content. This question is also included in our basic evaluation process.[238]

Figure 127: User Submission: Do the policies clearly indicate whether or not a user can create or upload content to the product?

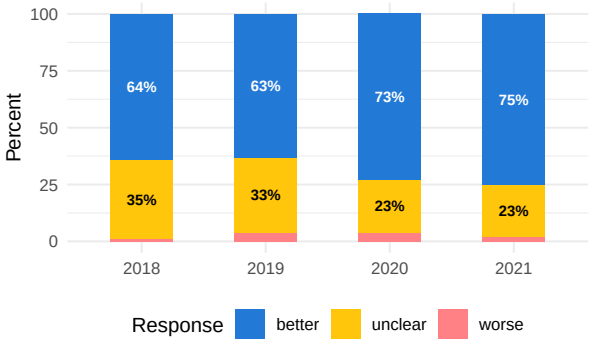


[238] *See* Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). *Privacy risks and harms*, San Francisco, CA: Common Sense Media.

Collection Consent

The Collection Consent evaluation question indicates whether the company requests opt-in consent from a user at the time personal information is collected with just-in-time or pop-up notices of what information will be collected and how it will be used. A company should provide notice to users in an easy-to-read format as a supplemental notice of the product's privacy policy at the point of collection in order to obtain better informed consent. A "better" response to this evaluation question indicates the product does obtain consent from a user at the time personal information is collected.[239,240,241,242]

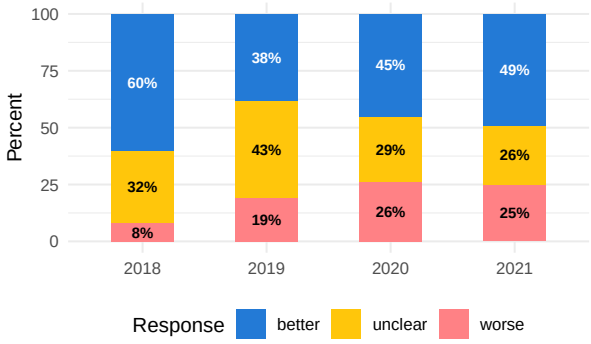
Figure 128: Collection Consent: Do the policies clearly indicate whether or not the vendor requests opt-in consent from a user at the time information is collected?



Complaint Notice

The Complaint Notice evaluation question indicates whether notification is provided to users if their account or content is restricted and if users can file a complaint with the company against the account or content restriction. A company should provide notice of a dispute resolution process for any account or content that is restricted and any available remedies. A "better" response to this evaluation question indicates the product does provide a process where users can file a complaint.[243,244,245,246,247,248,249,250,251]

Figure 129: Complaint Notice: Do the policies clearly indicate whether or not the vendor has a grievance or remedy mechanism for users to file a complaint after the vendor restricts or removes a user's content or account?



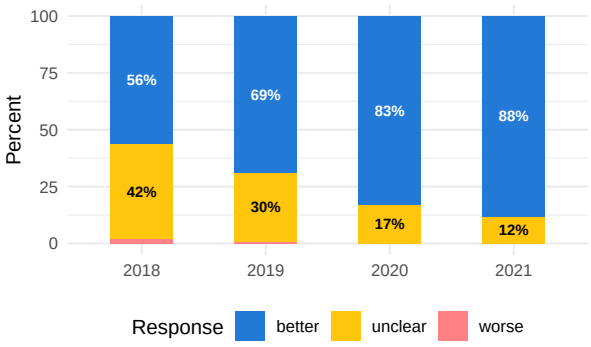
[239] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d).
[240] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.
[241] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(h).
[242] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(11), 6(1)(a), 7(1)-(2).

[243] *See* The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(c).
[244] *See* Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512(g)(2)(A).
[245] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(3).
[246] *See* General Data Protection Regulation (GDPR), Right to restriction of processing, Art. 18(1)(b).
[247] *See* General Data Protection Regulation (GDPR), Notification obligation regarding rectification or erasure of personal data or restriction of processing, Art. 19.
[248] General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art. 13(2)(d).
[249] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(e).
[250] *See* General Data Protection Regulation (GDPR), Right of access by the data subject, Art. 15(1)(f).
[251] *See* General Data Protection Regulation (GDPR), Right to an effective judicial remedy against a controller or processor, Art. 79(1), 79(2).

User Control

The User Control evaluation question indicates whether users can control the collection, use, or disclosure of their information in the product through changes in processing, privacy controls, or product settings. A company should provide information about a product's privacy settings and controls that users have with their personal information in a company's policies before users provide their data to a product, not afterward. A "better" response to this evaluation question indicates the product does provide users with privacy controls.

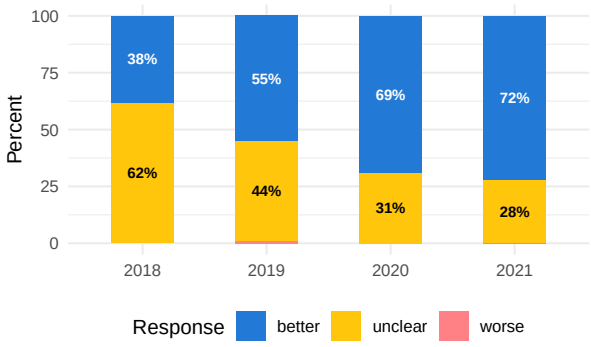
Figure 130: User Control: Do the policies clearly indicate whether or not a user can control the vendor or third party's use of their information through privacy settings?



Opt-Out Consent

The Opt-Out Consent evaluation question indicates whether a user can opt out or object to the company's processing of their information for a particular purpose such as selling data to third parties. A company should respect a user's informed consent and choice that the product must change its data collection, use, or disclosure practices of the personal information with respect to that user. A "better" response to this evaluation question indicates the product does provide users with the ability to give opt-out consent.[252,253,254,255,256,257,258]

Figure 131: Opt-Out Consent: 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?

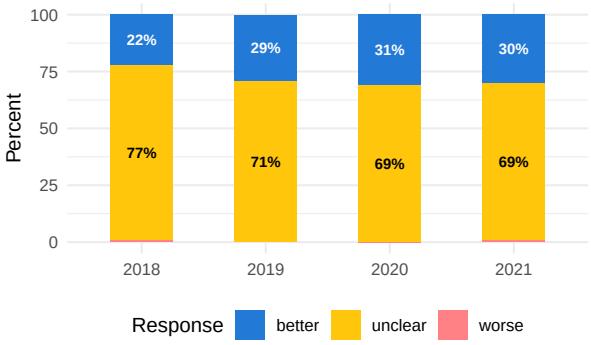


[252] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.3, 99.37.
[253] *See* Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.
[254] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(5).
[255] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.115(d).
[256] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.120(a), (d).
[257] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.135(a)-(b), (c)(6).
[258] *See* General Data Protection Regulation (GDPR), Art. 7(3), 13(2)(b), 14(2)(c), 15(1)(e), 21(1), 21(4).

Disclosure Request

The Disclosure Request evaluation question indicates whether users can obtain notice of all the categories of personal information the company shared with third parties for their own advertising or direct marketing purposes. A company should respond to a user's request and provide notice of whether a user's personal information was disclosed to third parties because there is an increased risk a user's personal information may be used for unintended purposes. A "better" response to this evaluation question indicates the product does provide notice if a user's data was disclosed to third parties for their own advertising or direct marketing purposes.[259,260,261,262,263,264,265,266]

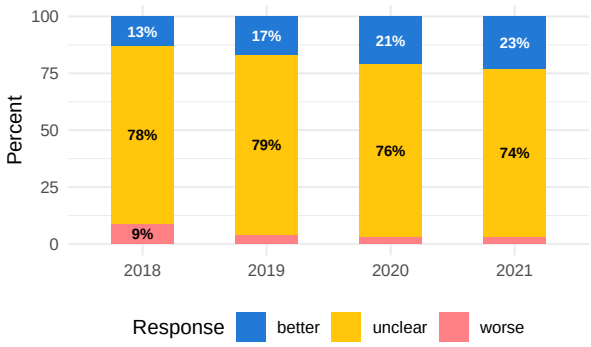
Figure 132: Disclosure Request: Do the policies clearly indicate whether or not a user can request the vendor to provide all the personal information the vendor has shared with third parties?



Disclosure Notice

The Disclosure Notice evaluation question indicates whether notification is provided to an affected user of a government or private company request for their personal information collected from the product. A company should disclose the number of legal requests for information received and situations when the company might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users.[267,268,269,270]

Figure 133: Disclosure Notice: Do the policies clearly indicate whether or not the vendor will provide the affected user, school, parent, or student with notice in the event the vendor receives a government or legal request for their information?



[259] *See* Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.

[260] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30(c)(1).

[261] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.115(c)(1)-(2).

[262] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(5)(B)(iii).

[263] *See* General Data Protection Regulation (GDPR), Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(1), 12(3), 12(4), 12(5), 12(7).

[264] *See* General Data Protection Regulation (GDPR), Right of access by the data subject, Art. 15(3).

[265] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, Art. 14(3)(a)-(c).

[266] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, Art. 14(5)(b).

[267] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(9)(ii).

[268] *See* California Electronic Communications Privacy Act, Cal. Pen. Code § 1546-1546.4.

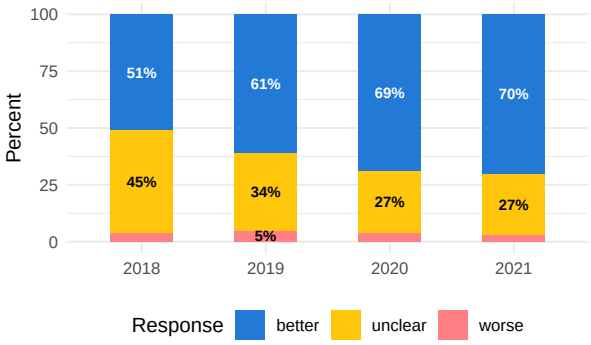
[269] *See* General Data Protection Regulation (GDPR), Right to erasure, Art. 17(1)(d).

[270] \textit{See General Data Protection Regulation (GDPR), Right to restriction of processing, Art. 18(1)(d).

Data Ownership

The Data Ownership evaluation question indicates whether the user retains copyright authorship or ownership rights to the user-generated content created or uploaded by the user to the product. A company should respect the intellectual property rights of the content creators using its service and allow users to extend copyright protection to their works. A "better" response to this evaluation question indicates the user retains any copyright authorship or ownership rights.[271,272]

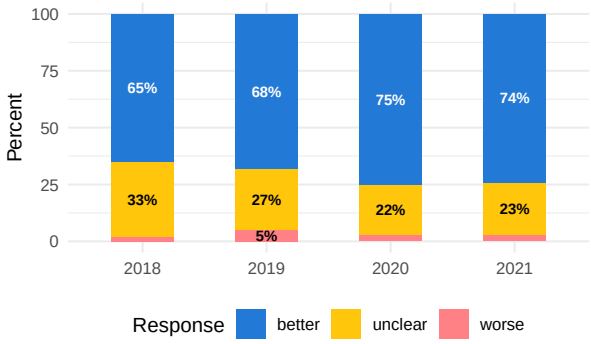
Figure 134: Data Ownership: Do the policies clearly indicate whether or not a student, educator, parent, or the school retains ownership to the Intellectual Property rights of the data collected or uploaded to the product?



Copyright License

The Copyright License evaluation question indicates whether the company may claim a copyright license to a user's information or content that is created in or uploaded to the service. A company should respect the intellectual property rights of the content creators using its service and only claim a copyright license to a user's work in order to display and distribute the works for the purpose of providing the service. A "better" response to this evaluation question indicates the company claims a copyright license to a user's information or content for use with the product.[273]

Figure 135: Copyright License: Do the policies clearly indicate whether or not the vendor may claim a copyright license to the data or content collected from a user?



[271] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(1).

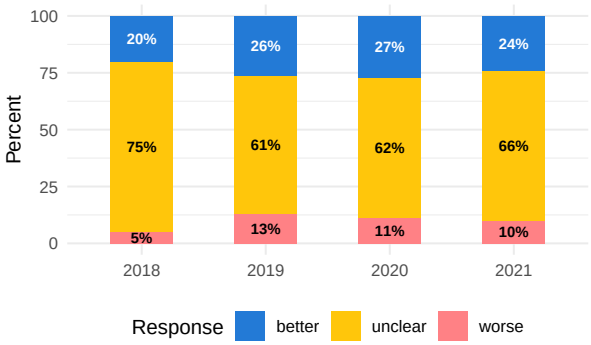
[272] *See* Copyright Act of 1976, 17 U.S.C. § 102.

[273] *See* Copyright Act of 1976, 17 U.S.C. § 106.

Copyright Limits

The Copyright Limits evaluation question indicates that the company limits or terminates its copyright license to a user's information or content created with the product in certain situations, such as when information or content is deleted from the service or after a specified period of account inactivity. A "better" response to this evaluation question indicates the company limits or terminates its copyright license.

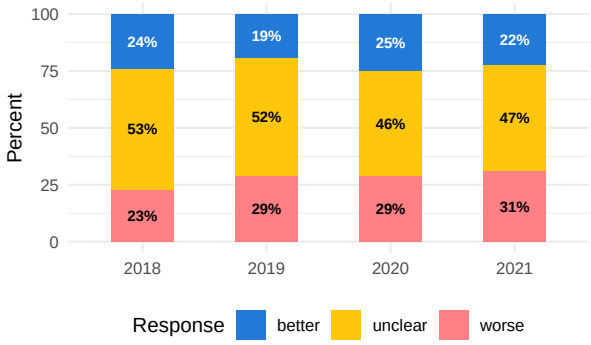
Figure 136: Copyright Limits: Do the policies clearly indicate whether or not the vendor limits its copyright license of a user's data?



Copyright Violation

The Copyright Violation evaluation question indicates whether the company has a process for receiving copyright infringement complaints and provides notification to users of alleged copyright infringement complaints of their content in order to appeal the complaint. A "better" response to this evaluation question indicates the company provides notice to a user of a copyright violation complaint and the opportunity to appeal.[274]

Figure 137: Copyright Violation: Do the policies clearly indicate whether or not the vendor provides notice to a user when their content is removed or disabled because of alleged infringement or other Intellectual Property violations?

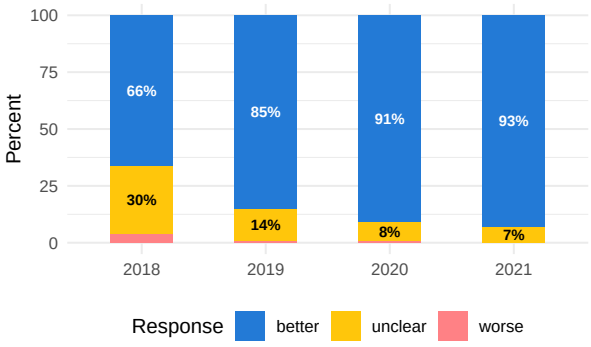


[274] *See* Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512(g)(2)(A).

Access Data

The Access Data evaluation question indicates that there is a process for a user to access and review their information through the product. A company should provide users with the ability to view and access the information and content in their account any time with the product to ensure fair and transparent processing of their data. A "better" response to this evaluation question indicates the product does provide a process for a user to access and review their information. This question is also included in our basic evaluation process.[275,276,277,278]

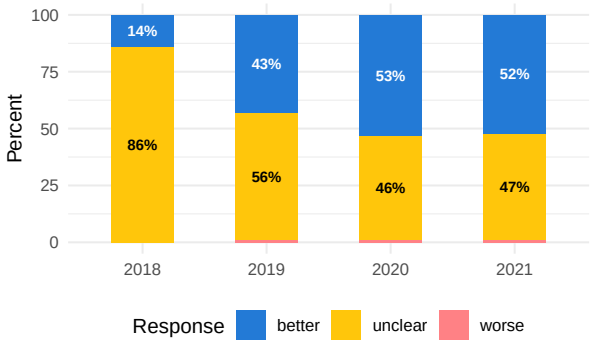
Figure 138: Access Data: Do the policies clearly indicate whether or not the vendor provides authorized individuals a method to access a user's personal information?



Restrict Access

The Restrict Access evaluation question indicates whether a process is available for restricting the processing of a user's information, or whether mechanisms are used (permissions, roles, or access controls, etc.) to restrict what data is accessible to specific users. A company should respond to a user's request to restrict access to their data if the accuracy of the data is disputed, or the processing is believed to be unlawful, but the user opposes the erasure of their personal data from the product. A "better" response to this evaluation question indicates the product does provide a process for restricting the processing of a user's information.[279,280,281,282,283]

Figure 139: Restrict Access: Do the policies clearly indicate whether or not the vendor provides mechanisms (permissions, roles, or access controls, etc.) to restrict what data are accessible to specific users?



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

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

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

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

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

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

[281] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art. 13(2)(b).

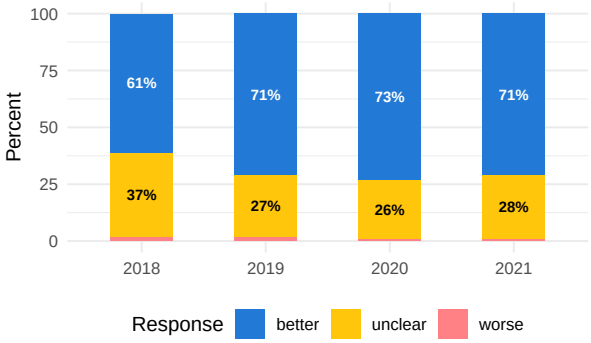
[282] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(c).

[283] *See* General Data Protection Regulation (GDPR), Right of access by the data subject, Art. 15(1)(e).

Review Data

The Review Data evaluation question indicates whether there is a process for educators in schools, parents at home, or eligible students to review their own personal information or the personal information of their students or children collected by the product. A "better" response to this evaluation question indicates the product does provide a process for educators or parents to review the personal information of their children and students.[284,285,286,287,288,289,290,291]

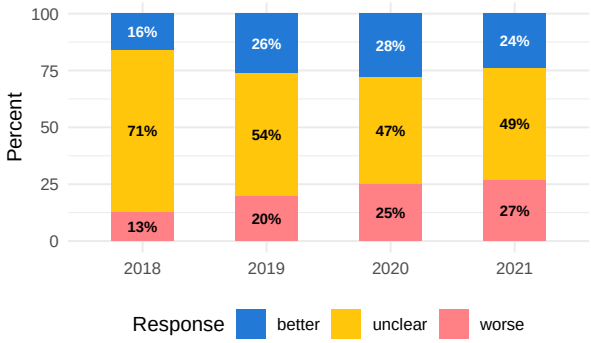
Figure 140: Review Data: Do the policies clearly indicate whether or not the vendor provides a process available for the school, parents, or eligible students to review student information?



Maintain Accuracy

The Maintain Accuracy evaluation question indicates whether the company has procedures to keep users' personal information accurate and up to date. A company should respond to a user's request to add, erase, or modify inaccurate personal information with additional regard to the purposes for which the data is processed. A "better" response to this evaluation question indicates the company does have procedures to keep users' personal information accurate.[292,293,294,295]

Figure 141: Maintain Accuracy: Do the policies clearly indicate whether or not the vendor takes steps to maintain the accuracy of data they collect and store?



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

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

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

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

[288] *See* California Privacy of Pupil Records, Cal. Ed. Code §§ 49073.1(b)(4), 49073.6(c).

[289] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.110(c)(5).

[290] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(1).

[291] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ah).

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

[293] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(e); *See also* 16 C.F.R. Part 312.8.

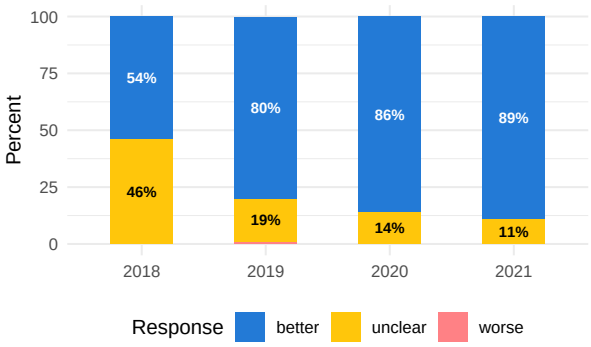
[294] *See* General Data Protection Regulation (GDPR), Principles relating to processing of personal data, Art. 5(1)(d).

[295] *See* General Data Protection Regulation (GDPR), Right to restriction of processing, Art. 18(1)(a).

Data Modification

The Data Modification evaluation question indicates whether there is a process for a user to access and modify their own information through the product. A company should provide users with the ability to view and edit the information and content in their account any time with the product to ensure fair and transparent processing of their data. A "better" response to this evaluation question indicates the product does have a process for a user to access and modify their own information. This question is also included in our basic evaluation process.[296,297,298,299]

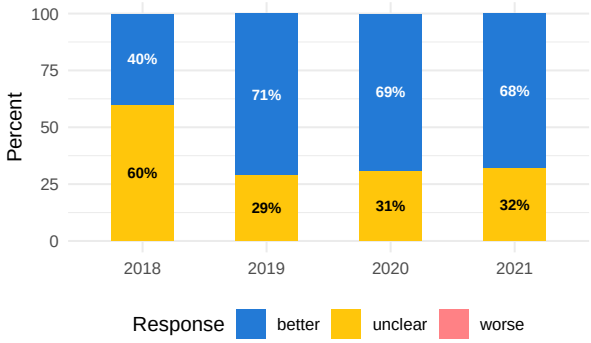
Figure 142: Data Modification: Do the policies clearly indicate whether or not the vendor provides authorized individuals with the ability to modify a user's inaccurate data?



Modification Process

The Modification Process evaluation question indicates whether there is a process for educators in schools, parents at home, or eligible students to review their own personal information or the personal information of their students or children collected by the product. A "better" response to this evaluation question indicates the product does provide a process for educators or parents to modify the personal information of their children and students.[300,301,302,303,304,305,306,307,308,309]

Figure 143: Modification Process: Do the policies clearly indicate whether or not the vendor provides a process for the schools, parents, or eligible students to modify inaccurate student information?



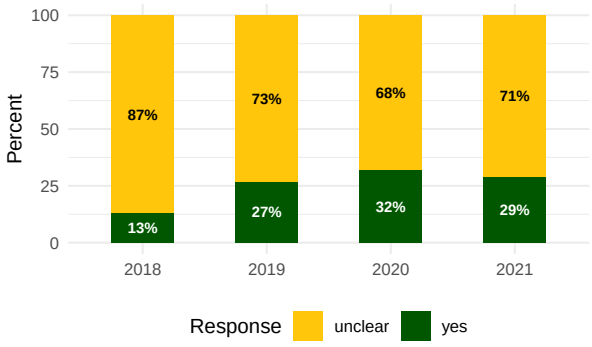
[296] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; 34 C.F.R. Part 99.20.
[297] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(2).
[298] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.106(a).
[299] *See* General Data Protection Regulation (GDPR), Right to rectification, Art. 16.

[300] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(c).
[301] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; 34 C.F.R. Part 99.20.
[302] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.5(a)(1).
[303] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(2).
[304] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(4).
[305] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.6(c).
[306] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.106(b)-(c).
[307] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(1).
[308] *see* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ak).
[309] *See* General Data Protection Regulation (GDPR), Notification obligation regarding rectification or erasure of personal data or restriction of processing, Art. 19.

Modification Notice

The Modification Notice evaluation question indicates whether the company provides a time frame in which they will modify a user's information after they have been provided notification of the request from the user. This evaluation question does not have a "better" or "worse" qualitative component.[310,311]

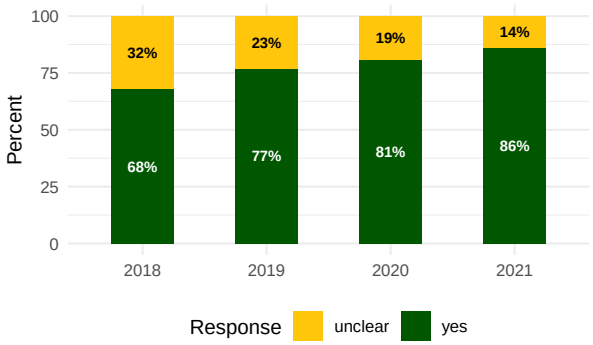
Figure 144: Modification Notice: Do the policies clearly indicate how long the vendor has to modify a user's inaccurate data after given notice?



Retention Policy

The Retention Policy evaluation question indicates whether the product has 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. A company should disclose how long different types of data are stored or retained by the company and if different retention periods apply to different users of the product. This evaluation question does not have a "better" or "worse" qualitative component.[312,313,314,315]

Figure 145: Retention Policy: Do the policies clearly indicate the vendor's data retention policy, including any data sunsets or any time-period after which a user's data will be automatically deleted if they are inactive on the product?



[310] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(2)(A).

[311] *See* General Data Protection Regulation (GDPR), Right to rectification, Art. 16.

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

[313] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(7).

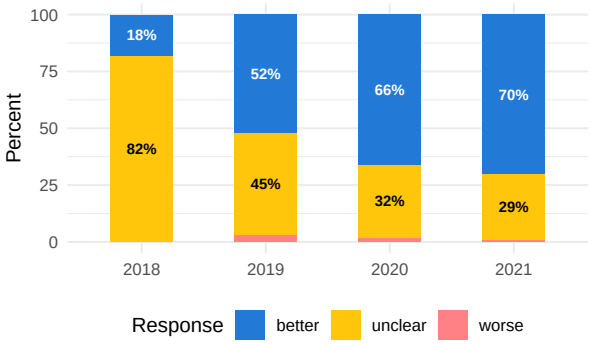
[314] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(a)(3).

[315] *See* General Data Protection Regulation (GDPR), Art. 13(2)(a), 14(2)(a), 15(1)(d).

Retention Limits

The Retention Limits evaluation question indicates whether the retention period for a user's data may be changed for a legitimate purpose or an inspection request is received, or other legal investigation request, or to protect the health and safety of other users of the product. A "better" response to this evaluation question indicates the product does provide notice if the retention period for a user's data may be changed.[316,317,318,319]

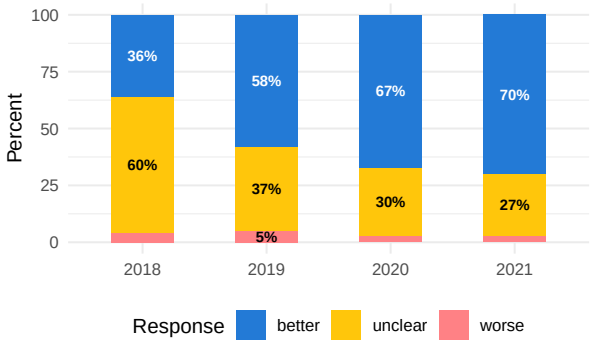
Figure 146: Retention Limits: Do the policies clearly indicate whether or not the vendor will limit the retention of a user's data unless a valid request to inspect data is made?



Deletion Purpose

The Deletion Purpose evaluation question indicates whether a user's personal information will be deleted when no longer necessary for the purpose in which it was collected to provide the service. A company should delete a user's data after a specified time period in accordance with its retention policy, such as the end of a semester, a period of inactivity on the account, or termination by the user of the user's account. A "better" response to this evaluation question indicates a user's personal information will be deleted when no longer necessary.[320,321,322,323]

Figure 147: Deletion Purpose: Do the policies clearly indicate whether or not the vendor will delete a user's personal information when the data are no longer necessary to fulfill its intended purpose?

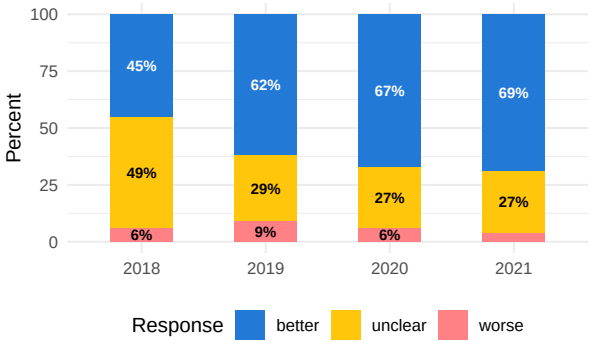


[316] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.7(a).
[317] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.105(c)(2), (d)(1)-(8).
[318] *See* General Data Protection Regulation (GDPR), Principles relating to processing of personal data, Art. 5(1)(e).
[319] *See* General Data Protection Regulation (GDPR), Right to restriction of processing, Art. 18(1)(c).
[320] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10.
[321] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(7).
[322] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(a)(3).
[323] *See* General Data Protection Regulation (GDPR), Right to erasure, Art. 17(1)(a).

Account Deletion

The Account Deletion evaluation question indicates whether a user has the ability to terminate their account with the product by canceling their service with the company, deleting their account through the product, or removing the product from their device. A company should delete all personal data from the user's account upon termination. A "better" response to this evaluation question indicates the product does provide a user with the ability to terminate their account with the product.[324,325,326,327]

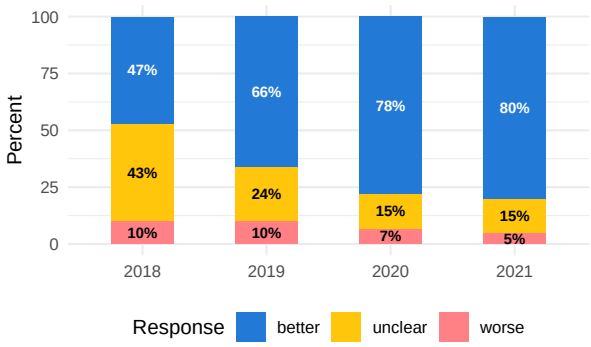
Figure 148: Account Deletion: Do the policies clearly indicate whether or not a user's data are deleted upon account cancellation or termination?



User Deletion

The User Deletion evaluation question indicates that there is a process for a user to access and delete their information through the product. A company should provide users with the ability to view and erase the information and content in their account any time with the product to ensure fair and transparent processing of their data. A "better" response to this evaluation question indicates the product does provide a process for a user to access and delete their information through the product.[328,329,330,331]

Figure 149: User Deletion: Do the policies clearly indicate whether or not a user can delete all of their personal and non-personal information from the vendor?



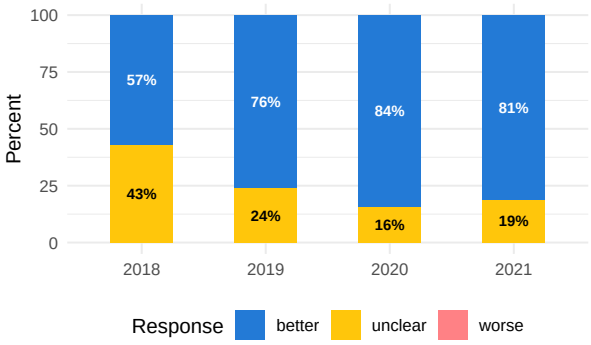
[324] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10.
[325] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; 34 C.F.R. Part 99.20.
[326] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.5(a)(1).
[327] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(d)(2).

[328] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(2).
[329] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.
[330] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.105(a).
[331] *See* General Data Protection Regulation (GDPR), Right to erasure, Art. 17(2).

Deletion Process

The Deletion Process evaluation question indicates whether there is a process for educators in schools, parents at home, or eligible students to review and delete their own personal information or the personal information of their students or children collected by the product. A company should provide managed account controls or disclose contact information where parents and educators can request to delete data of children or students. A "better" response to this evaluation question indicates the product does provide a process for educators or parents to delete the personal information of their children and students. This question is also included in our basic evaluation process.[332,333,334,335,336,337,338,339]

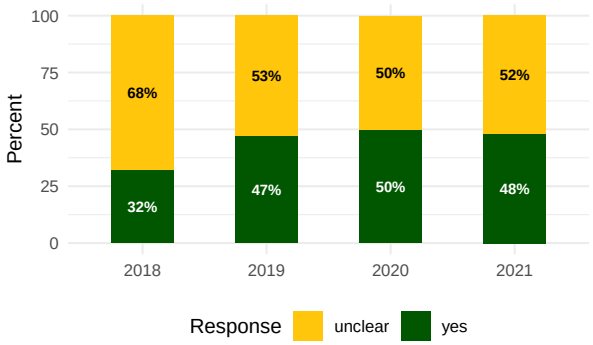
Figure 150: Deletion Process: Do the policies clearly indicate whether or not the vendor provides a process for the school, parent, or eligible student to delete a student's personal information?



Deletion Notice

The Deletion Notice evaluation question indicates whether the company provides a time frame in which they will delete a user's information from the product after they have been provided notification of the request from the user. This evaluation question does not have a "better" or "worse" qualitative component.[340,341,342]

Figure 151: Deletion Notice: Do the policies clearly indicate how long the vendor may take to delete a user's data after given notice?



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

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

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

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

[336] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.105(a)-(c)(1)-(3).

[337] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(1).

[338] *see* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ak).

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

[340] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(2)(A).

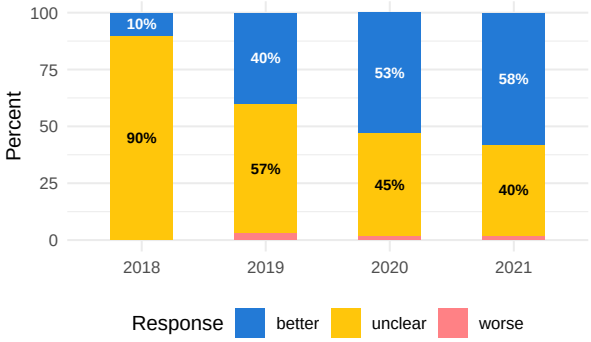
[341] *See* General Data Protection Regulation (GDPR), Right to rectification, Art. 16.

[342] *See* General Data Protection Regulation (GDPR), Right to erasure, Art. 17(1).

User Export

The User Export evaluation question indicates whether a user can export or download their data from the product, including any user-created content on the product in a structured data format for use with another product. A "better" response to this evaluation question indicates the product does provide a process for a user can export or download their data from the product.[343,344,345,346]

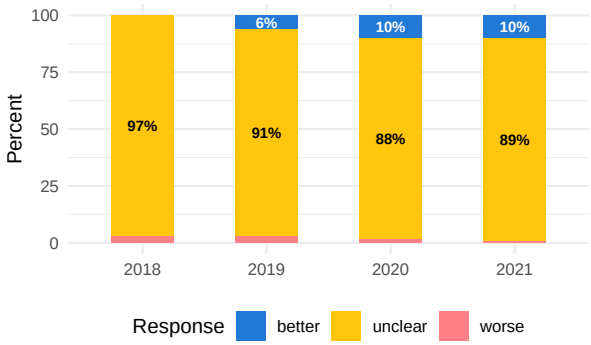
Figure 152: User Export: Do the policies clearly indicate whether or not a user can export or download their data, including any user created content on the product?



Legacy Contact

The Legacy Contact evaluation question indicates that the product provides a process to assign a managed account owner or authorized trusted contact if the account becomes inactive in order to retain access to the user's information and content in the event of the user's impairment or death. A "better" response to this evaluation question indicates the product does provide a process to assign a managed account owner or authorized trusted contact.[347]

Figure 153: Legacy Contact: Do the policies clearly indicate whether or not a user may assign an authorized account manager or legacy contact to access and download their data?



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

[344] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(2).

[345] *See* General Data Protection Regulation (GDPR), Art. 13(2)(b), 14(2)(c), 20(1)-(2).

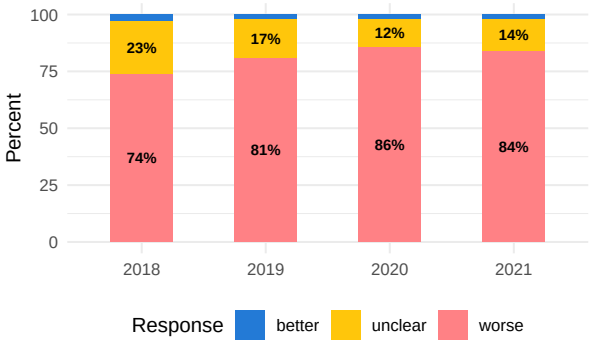
[346] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.130(a)(2)(A), (a)(3)(B)(iii).

[347] *See* California Revised Uniform Fiduciary Access to Digital Assets Act, Cal. Prob. Code § 870-884.

Transfer Data

The Transfer Data evaluation question indicates whether a user's information may be transferred as an asset to a successor third party in the event of a merger, acquisition, or bankruptcy. A company should carefully consider whether to transfer a user's personal information to a third party in exchange for monetary value because of the increased risk the personal information may be used for unintended purposes. A "better" response to this evaluation question indicates a user's information will not be transferred as an asset to a successor third-party company. This question is also included in our basic evaluation process.[348,349,350,351,352,353,354]

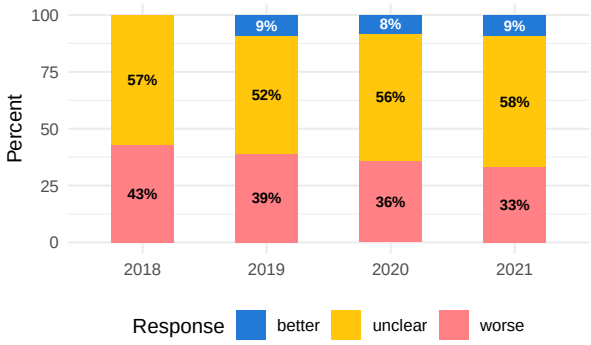
Figure 154: Transfer Data: Do the policies clearly indicate whether or not the vendor can transfer a user's data in the event of the vendor's merger, acquisition, or bankruptcy?



Data Assignment

The Data Assignment evaluation question indicates that the company will provide notification to users before assigning its rights and obligations of the product's privacy policies to a third-party company. A company should provide notice to users in the event the company assigns its ownership of the product to a third party because the change in control of a user's data could increase the risk that personal information is used for unintended purposes. A "better" response to this evaluation question indicates the company will not assign its rights and obligations of the product to a third-party company.

Figure 155: Data Assignment: Do the policies clearly indicate whether or not the vendor can assign its rights or delegate its duties under the policies to a successor vendor without notice or consent to the user?

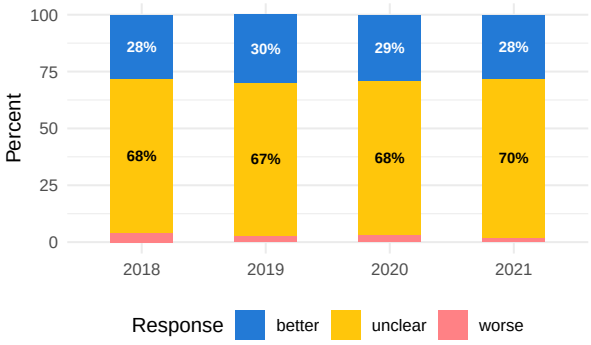


[348] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.3, 99.37.
[349] *See* Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.
[350] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(5).
[351] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ad)(2)(C).
[352] *See* General Data Protection Regulation (GDPR), Art. 7(3), 13(2)(b), 14(2)(c), 15(1)(e), 21(1), 21(4).
[353] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[354] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).

Transfer Notice

The Transfer Notice evaluation question indicates whether the company provides notice to users before a user's information may be transferred as an asset to a successor third party in the event of a merger, acquisition, or bankruptcy. A company should provide notice to users in the event their personal information is transferred to a third party to allow the user to make an informed decision whether or not to continue using the product. A "better" response to this evaluation question indicates the company provides notice to users before a user's information may be transferred as an asset to a successor third-party company.

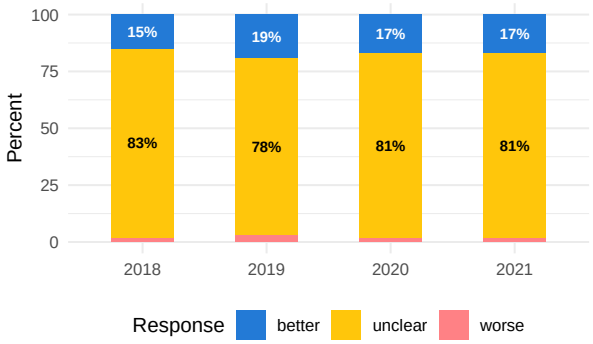
Figure 156: Transfer Notice: Do the policies clearly indicate whether or not the vendor will notify users of a data transfer to a third-party successor, in the event of a vendor's bankruptcy, merger, or acquisition?



Delete Transfer

The Delete Transfer evaluation question indicates whether notice is provided to users that they may delete their data before a user's information is transferred as an asset to a successor third party in the event of a merger, acquisition, or bankruptcy. A company should provide notice and allow users to delete their data as a best practice in the event their personal information is transferred to a third party to allow the user to make an informed decision whether or not to continue using the product. A "better" response to this evaluation question indicates users may delete their data before a user's information is transferred as an asset to a successor third-party company.

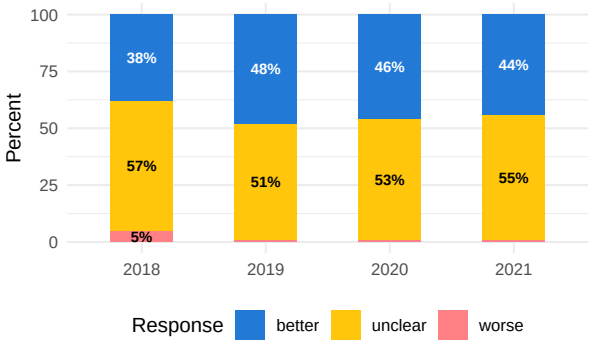
Figure 157: Delete Transfer: Do the policies clearly indicate whether or not a user can request to delete their data prior to its transfer to a third-party successor in the event of a vendor bankruptcy, merger, or acquisition?



Contractual Limits

The Contractual Limits evaluation question indicates whether the company places contractual obligations or restrictions on the use of users' data on the successor third party in the event of a merger, acquisition, or bankruptcy. A successor third party should adopt the company's privacy policies for the product and process data in accordance with the same privacy practices that users provided their informed consent in order to prevent users' personal information from being used for unintended purposes. A "better" response to this evaluation question indicates the company places contractual obligations or restrictions on the use of users' data on the successor third-party company.[355,356,357]

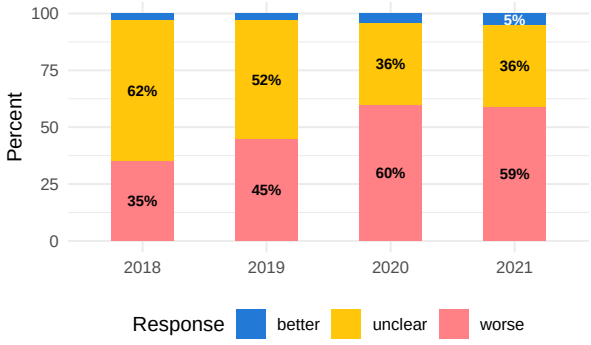
Figure 158: Contractual Limits: Do the policies clearly indicate whether or not the third-party successor of a data transfer is contractually required to provide the same privacy compliance required of the vendor?



Verify Identity

The Verify Identity evaluation question indicates that additional personal information is collected from a user by the product to verify their identity with a government-issued identification or with other forms of identification that could be connected to their offline identity. A company should not require users to provide sensitive information about their offline identity unless necessary to protect the personal information of the user for which the request to access, modify, delete, or export their personal information and requires the extra security of verifying their identity. A "better" response to this evaluation question indicates the product does not require additional personal information to be collected from a user to verify their identity.[358,359,360,361,362]

Figure 159: Verify Identity: Do the policies clearly indicate whether or not the vendor or vendor-authorized third party verifies a user's identity with personal information?



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

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

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

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

[359] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(i)-(iv); *See also* 15 U.S.C. § 6501(9).

[360] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.130(a)(7).

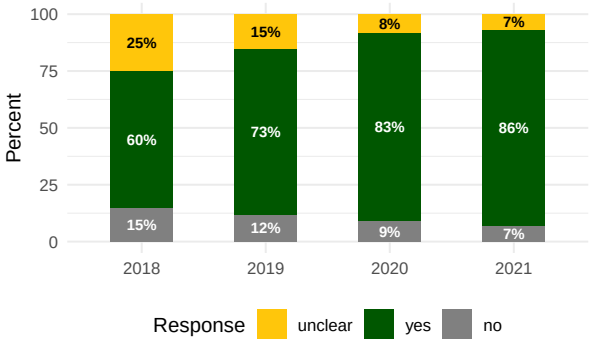
[361] *See* General Data Protection Regulation (GDPR), Conditions Applicable to Child's Consent in Relation to Information Society Services, Art. 8(2).

[362] *See* General Data Protection Regulation (GDPR), Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(6).

Account Required

The Account Required evaluation question indicates whether the product allows users to create an account to protect their personal information. A product should allow users to create an account and authenticate it in order to provide user controls to access, edit, delete, and export their information as well as settings to control how their data is used. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.

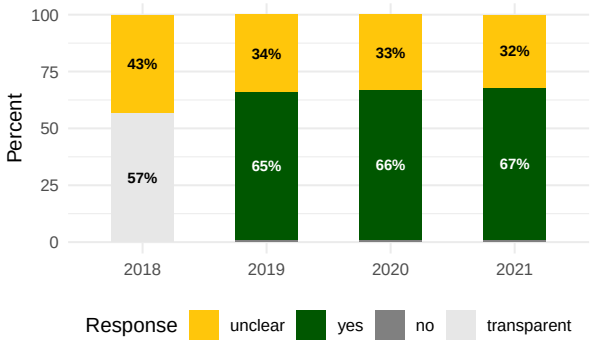
Figure 160: Account Required: Do the policies indicate whether or not the vendor requires a user to create an account with a username and password in order to use the product?



Managed Account

The Managed Account evaluation question indicates whether parental controls or other managed settings are available for parents, teachers, schools or districts to access, review, edit, and delete the personal information of children or students. A company should create a managed account or child profile if the intended audience of the product includes children or students because it allows the product to provide better privacy-protecting data collection and use practices to users who use the managed account or profile. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.[363]

Figure 161: Managed Account: Do the policies clearly indicate whether or not the vendor provides user managed accounts for a parent, teacher, school or district?

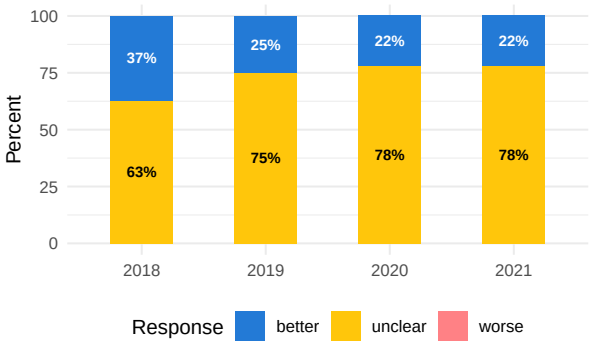


[363] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.10, 99.20, 99.5(a)(1).

Two-Factor Protection

The Two-Factor Protection evaluation question indicates whether user accounts can be protected with additional two-factor authentication for better security through the use of mobile SMS or a third-party authenticator service. A "better" response to this evaluation question indicates the product does provide user accounts with additional two-factor authentication.

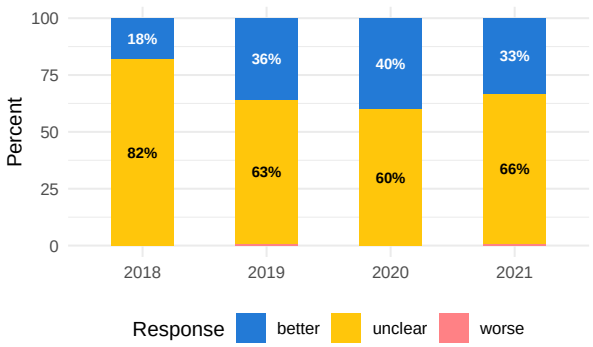
Figure 162: Two-Factor Protection: Do the policies clearly indicate whether or not the security of a user's account is protected by two-factor authentication?



Security Agreement

The Security Agreement evaluation question indicates whether contractual obligations are imposed on third-party service providers to require additional security protections for users' personal information. A company should put in place contractual obligations that require third parties to use the same reasonable security practices as the product in accordance with the company's privacy policy. Without contractual requirements on third-party security practices of data collected from children and students, parents and educators cannot reasonably expect that the privacy provisions outlined in the product's policies will be honored by third parties that have access to personal data. A "better" response to this evaluation question indicates the company requires additional security contractual obligations on third-party service providers.[364,365,366,367,368,369]

Figure 163: Security Agreement: Do the policies clearly indicate whether or not a third party with access to a user's information is contractually required to provide the same level of security protections as the vendor?

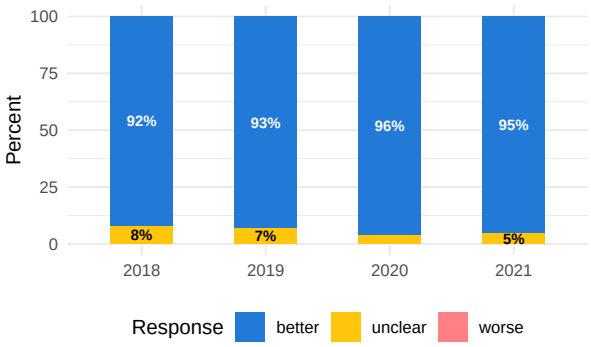


[364] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.
[365] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii).
[366] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(iii).
[367] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).
[368] *See* General Data Protection Regulation (GDPR), Processor, Art. 28(1).
[369] *See* General Data Protection Regulation (GDPR), Security of processing, Art. 32(4).

Reasonable Security

The Reasonable Security evaluation question indicates whether any security protections are in place with the product for users' information based on industry standards and best practices. A company should use various technologies and security processes that are continuously updated to protect users' personal information collected by the product from unauthorized access. A "better" response to this evaluation question indicates the product does provide security protections. This question is also included in our basic evaluation process.[370,371,372,373,374,375,376,377]

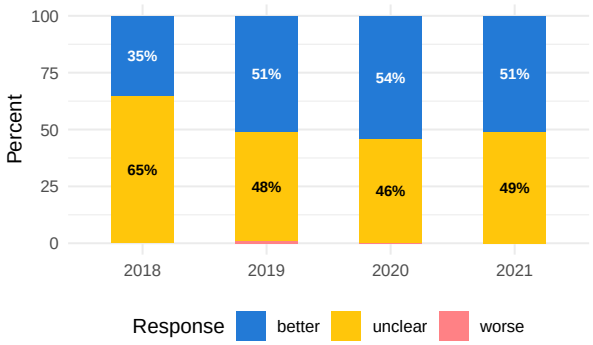
Figure 164: Reasonable Security: Do the policies clearly indicate whether or not reasonable security standards are used to protect the confidentiality of a user's personal information?



Employee Access

The Employee Access evaluation question indicates that the company implements physical access controls or limits employee access to user information only on a need-to-know basis to better protect users from unauthorized access of their data for unintended purposes. A "better" response to this evaluation question indicates the company does implement physical access controls or limits employee access to user information.[378,379]

Figure 165: Employee Access: Do the policies clearly indicate whether or not the vendor implements physical access controls or limits employee access to user information?



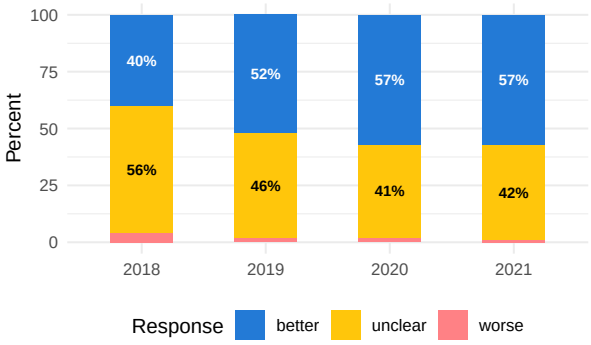
[370] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(e); *See also* 16 C.F.R. Part 312.8.
[371] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii).
[372] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(d)(1).
[373] *See* California Data Breach Notification Requirements, Cal. Civ. Code §1798.81.5.
[374] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).
[375] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100(e).
[376] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(e)(2)-(3), (ac).
[377] *See* General Data Protection Regulation (GDPR), Art. 5(1)(f), 32(1)(b), 32(2).

[378] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).
[379] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.135(c)(3).

Transit Encryption

The Transit Encryption evaluation question indicates that a user's personal information collected by the product is transmitted in an encrypted format such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). A company should not collect and transmit personal information over the internet without encryption because the personal information could be intercepted by unauthorized individuals which increases the risk a user's data is used for unintended purposes. A "better" response to this evaluation question indicates the product does encrypt user information transmitted over the internet. This question is also included in our basic evaluation process.[380,381,382]

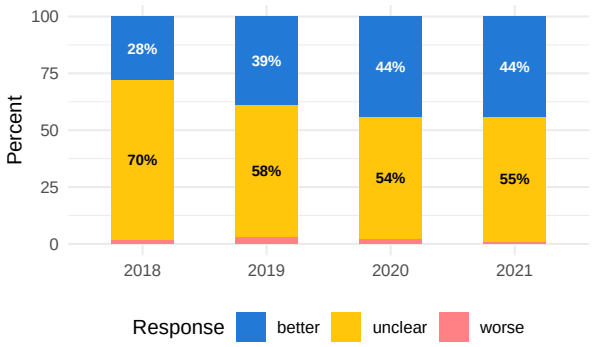
Figure 166: Transit Encryption: Do the policies clearly indicate whether or not all data in transit is encrypted?



Storage Encryption

The Storage Encryption evaluation question indicates that a user's data is stored in the company's data servers in an encrypted format. A company should not collect and store a user's personal information without encryption because the personal information could be accessed by unauthorized individuals or disclosed in a data breach, which increases the risk that a user's data is used for unintended purposes. A "better" response to this evaluation question indicates the product does encrypt user data stored on the company's servers. This question is also included in our basic evaluation process.[383,384]

Figure 167: Storage Encryption: Do the policies clearly indicate whether or not all data at rest is encrypted?



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

[381] *See* California Data Breach Notification Requirements, Cal. Civ. Code §1798.81.5.

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

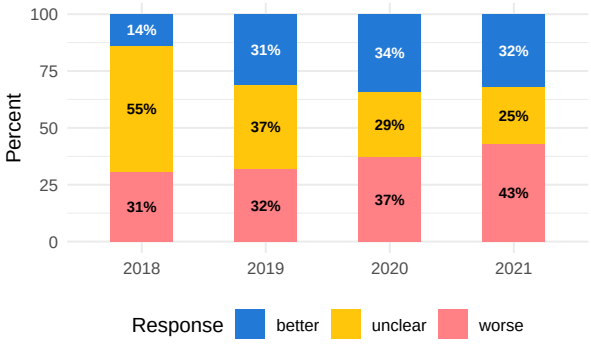
[383] *See* California Data Breach Notification Requirements, Cal. Civ. Code §1798.81.5.

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

Data Control

The Data Control evaluation question indicates that the company stores data only in the country where the company primarily operates under its control. A company should maintain its users' data in its home jurisdiction because other countries may have privacy and data protection laws that are potentially more or less protective than the laws of the country where a user's data is stored. A "better" response to this evaluation question indicates the company stores data only in its home country.[385,386,387,388,389,390]

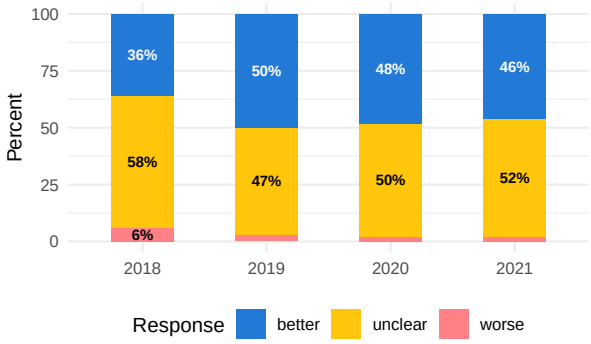
Figure 168: Data Control: Do the policies clearly indicate whether or not personal information is stored outside the control of the vendor?



Breach Notice

The Breach Notice evaluation question indicates that in the event of a data breach, if unencrypted collected information is disclosed to unauthorized individuals, the company will provide notice to any users affected. A company should provide notice to users in the event their data is disclosed in a data breach because there is an increased risk the data may be used for unintended purposes. A "better" response to this evaluation question indicates the product does provide notice to users in the event of a data breach. This question is also included in our basic evaluation process.[391,392,393,394,395]

Figure 169: Breach Notice: Do the policies clearly indicate whether or not the vendor provides notice in the event of a data breach to affected individuals?



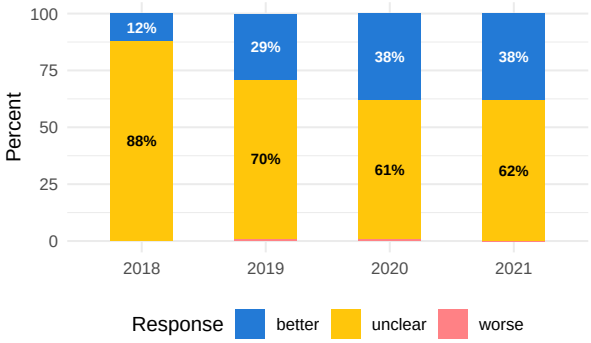
[385] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(e); *See also* 16 C.F.R. Part 312.8.
[386] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.
[387] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(iii).
[388] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(1).
[389] *See* General Data Protection Regulation (GDPR), Security of processing, Art. 32(1)(c).
[390] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(B).

[391] *See* California Data Breach Notification Requirements, Cal. Civ. Code §§ 1798.29, 1798.29(h)(4), 1798.82.
[392] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(6).
[393] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.150(a)(1)-(2).
[394] *See*General Data Protection Regulation (GDPR), Definitions, Art. 4(12), 33(1)-(5), 34(1)-(3).
[395] National Conference of State Legislatures, *Security Breach Notification Laws* (Apr. 5, 2021), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Security Audit

The Security Audit evaluation question indicates whether the company has internal or third-party privacy or security staff assessments or audits to ensure user data is secure. A company should implement occasional privacy and security assessments that are continuously updated to protect users' personal information collected by the product from unauthorized access. A "better" response to this evaluation question indicates the company has internal or third-party privacy or security staff assessments or audits.[396,397,398]

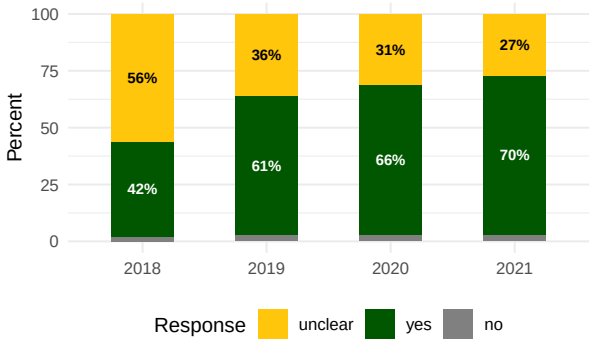
Figure 170: Security Audit: Do the policies clearly indicate whether or not the data privacy or security practices of the vendor are internally or externally audited to ensure compliance?



Safe Interactions

The Safe Interactions evaluation question indicates whether users can have social interactions with trusted or other known users, such as with students in the same classroom or school, or friends they know in real life. A company should only provide safe interactions for children and students with users that they already know or have a real-life relationship with offline to prevent inappropriate conversations with adults that could cause emotional or physical harm. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.[399,400]

Figure 171: Safe Interactions: Do the policies clearly indicate whether or not a user can interact with trusted users?



[396] *See* General Data Protection Regulation (GDPR), Principles relating to processing of personal data, Art. 5(2).

[397] *See* General Data Protection Regulation (GDPR), Responsibility of the controller, Art. 24(1), Art. 24(2).

[398] *See* General Data Protection Regulation (GDPR), Security of processing, Art. 32(1)(d).

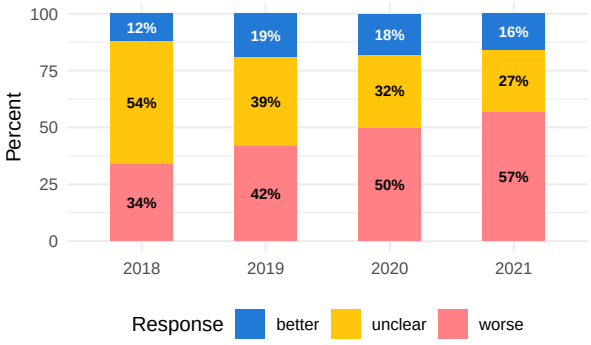
[399] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

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

Unsafe Interactions

The Unsafe Interactions evaluation question indicates whether any users can have social interactions with other unknown users, such as other users on the product who may be adults or children. A company should only provide unsafe interactions between adults to prevent inappropriate conversations between adults and children that could cause emotional or physical harm. A "better" response to this evaluation question indicates the product does not provide social interactions with other unknown users.[401,402]

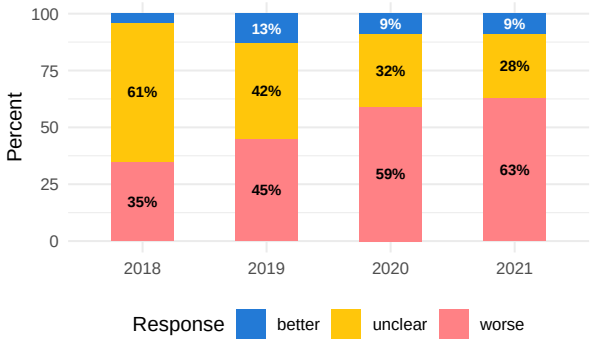
Figure 172: Unsafe Interactions: Do the policies clearly indicate whether or not a user can interact with untrusted users?



Share Profile

The Share Profile evaluation question indicates whether the user's profile information on the product can be shared with other users for social interactions. A company should limit the types of profile information that can be shared with other users or publicly with privacy controls to prevent inadvertent disclosure of a user's identity that could cause emotional or physical harm. A "better" response to this evaluation question indicates the product does not disclose a user's profile information to other users for social interactions.[403]

Figure 173: Share Profile: Do the policies clearly indicate whether or not information must be shared or revealed by a user in order to participate in social interactions?



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

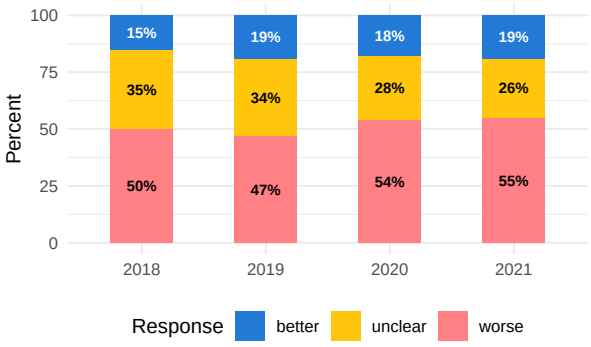
[402] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(2).

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

Visible Data

The Visible Data evaluation question indicates whether a user's personal information may be made publicly available on the product to other unknown users, or publicly available online to anyone. A company should use privacy-by-design principles with default privacy controls that use the most privacy-protecting settings for a user's personal data that set visibility to "``private" on the product which allows the user to change the visibility as needed. A company should also limit the types of profile information of children or students that can be shared with other users or publicly to prevent inadvertent disclosure of a user's identity that could cause emotional or physical harm. A "better" response to this evaluation question indicates the product does not allow a user's information to be made publicly available. This question is also included in our basic evaluation process.[404,405]

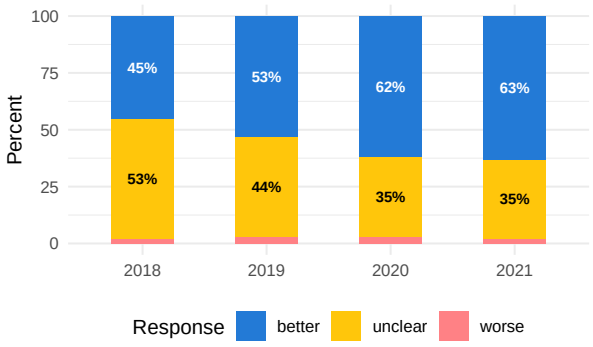
Figure 174: Visible Data: Do the policies clearly indicate whether or not a user's personal information can be displayed publicly in any way?



Control Visibility

The Control Visibility evaluation question indicates whether a user can control how their personal information is displayed to others on the product or elsewhere online. A company should limit the types of profile information of children or students that can be shared with other users or publicly with privacy controls to prevent inadvertent disclosure of a user's identity that could cause emotional or physical harm. A "better" response to this evaluation question indicates a user can control how their personal information is displayed to others.

Figure 175: Control Visibility: Do the policies clearly indicate whether or not a user has control over how their personal information is displayed to others?



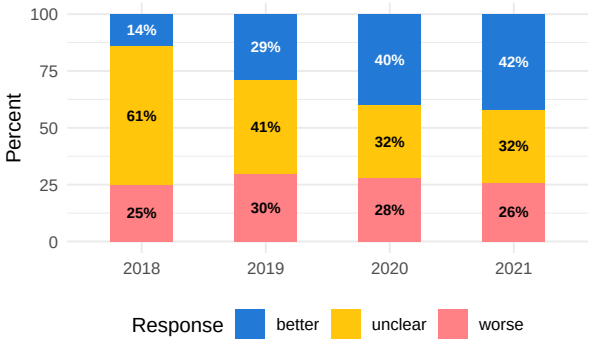
[404] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

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

Monitor Content

The Monitor Content evaluation question indicates that the company has a process to review, screen, or monitor user-created content for inappropriate content. A company should have a content-moderation management system in place to prevent age-inappropriate content from being shared between adults and children that could cause emotional or physical harm. A "better" response to this evaluation question indicates the company has a process to review, screen, or monitor user-created content for inappropriate content.

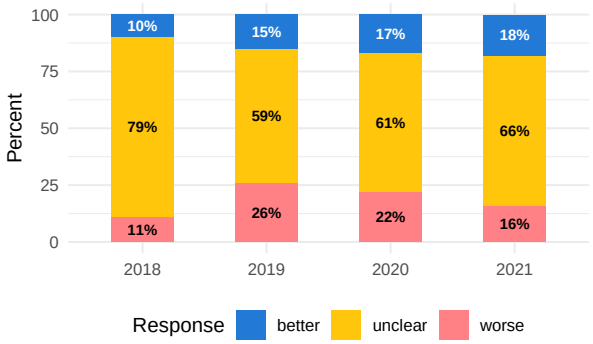
Figure 176: Monitor Content: Do the policies clearly indicate whether or not the vendor reviews, screens, or monitors user-created content?



Filter Content

The Filter Content evaluation question indicates that all personal information is deleted by the company from a child's or student's postings on the product before it is made public or available to other users. A company should have a content-filtering system in place to prevent personal information from children and students from being shared publicly or between adults and children that could cause emotional or physical harm. A "better" response to this evaluation question indicates the product does delete any personal information in a child's or student's posting on the product before it is made public or available to other users. This question is also included in our basic evaluation process.[406]

Figure 177: Filter Content: Do the policies clearly indicate whether or not the vendor takes reasonable measures to delete all personal information from a user's postings before they are made publicly visible?

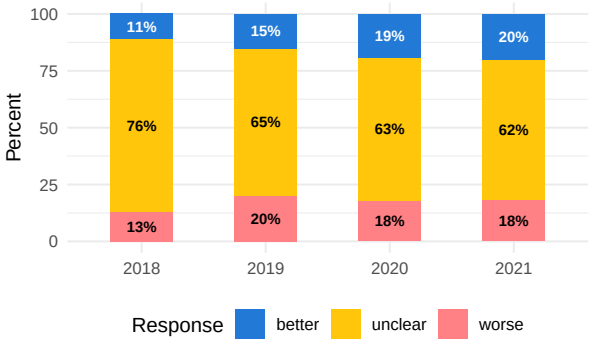


[406] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

Moderating Interactions

The Moderating Interactions evaluation question indicates whether the company monitors and filters social interactions between users on the product. A company should have a social interaction filtering system in place to prevent personal information from children and students from being shared between adults and children that could cause emotional or physical harm. A "better" response to this evaluation question indicates the company monitors and filters social interactions between users on the product. This question is also included in our basic evaluation process. [407]

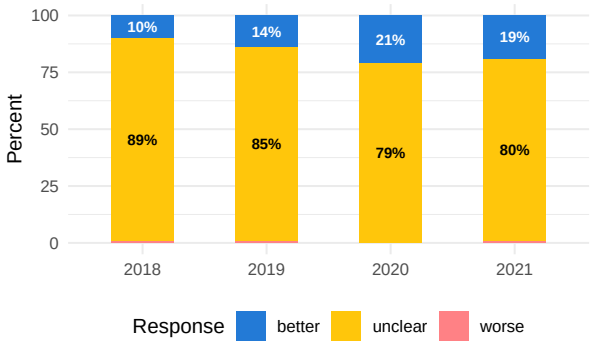
Figure 178: Moderating Interactions: Do the policies clearly indicate whether or not social interactions between users of the product are moderated?



Log Interactions

The Log Interactions evaluation question indicates that social interactions between users on the product are logged by the company for safety purposes. A company that provides social interactions between users should log interactions only for a specified period of time to prevent inappropriate conversations between adults and children that could cause emotional or physical harm. However, logging of children's or 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. A "better" response to this evaluation question indicates the product does log social interactions on the product for safety purposes.

Figure 179: Log Interactions: Do the policies clearly indicate whether or not social interactions are logged by the vendor and are available for review or audit?

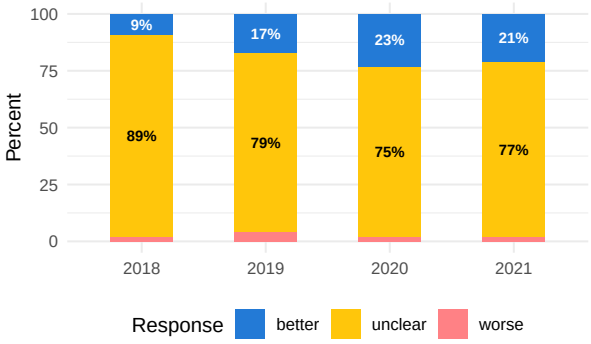


[407] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

Block Content

The Block Content evaluation question indicates that there is a process for the user, parent, or educator to temporarily or permanently block inappropriate content on the product from being displayed to children and students. A company should have a content-filtering system in place to prevent children and students from being exposed to obscene or inappropriate content that could cause emotional or physical harm. A "better" response to this evaluation question indicates there is a process for the user, parent, or educator to temporarily or permanently block inappropriate content on the product.[408,409]

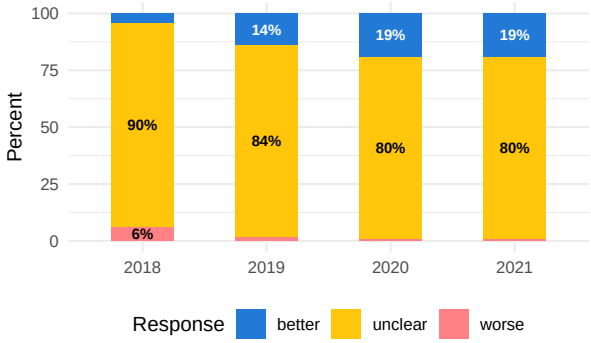
Figure 180: Block Content: Do the policies clearly indicate whether or not an educator, parent, or a school has the ability to filter or block inappropriate content or social interactions?



Report Abuse

The Report Abuse evaluation question indicates that there is a process for the user, parent, or educator to temporarily or permanently block specific users on the product from displaying content or engaging in social interactions with other children and students. The ability to report abuse and cyberbullying is becoming increasingly important to teachers and parents in order to protect children who are spending more time online both in and out of school. A company should have a cyberbullying- or abuse-reporting mechanism in place to prevent children and students from being exposed to abuse that could cause emotional or physical harm. A "better" response to this evaluation question indicates there is a process for the user, parent, or educator to temporarily or permanently block specific users on the product.[410]

Figure 181: Report Abuse: Do the policies clearly indicate whether or not a user can report abusive behavior, or cyberbullying?



[408] *See* Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5)(B).

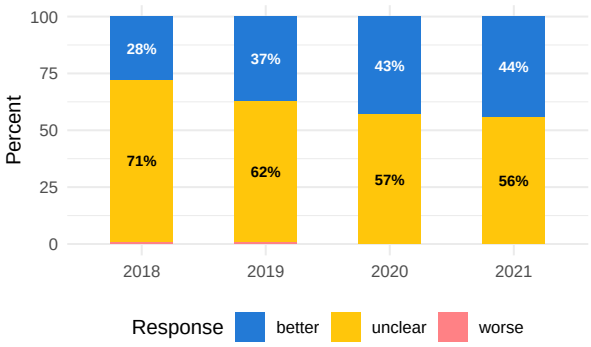
[409] *See* The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(d).

[410] *See* Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5)(B).

Safe Tools

The Safe Tools evaluation question indicates that the company provides links to third-party resources to help consumers, parents, and educators learn more about how to better protect their privacy on the product and the privacy of their children and students. A "better" response to this evaluation question indicates the company does prioritize the safety and privacy of its users with links to third-party resources to learn more how to become a better digital citizen and protect themselves online.[411,412,413]

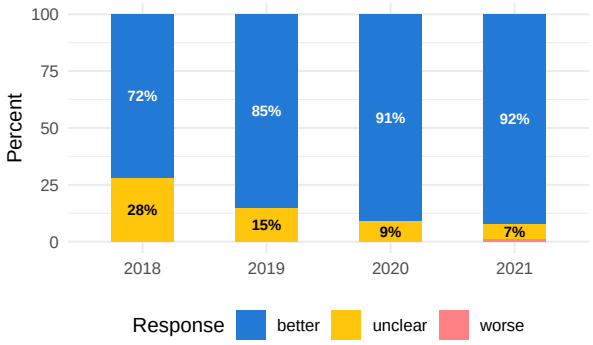
Figure 182: Safe Tools: Do the policies clearly indicate whether or not the vendor provides tools and processes that support safe and appropriate social interactions on the product?



Service Messages

The Service Messages evaluation question indicates that users may receive non-marketing communications from the company by email or mobile notifications to provide notice of important updates, service announcements, or changes to the policies or practices of the product. A "better" response to this evaluation question indicates the product does send non-marketing communications to provide notice of important updates, service announcements, or changes to the policies.

Figure 183: Service Messages: Do the policies clearly indicate whether or not a user will receive service- or administrative-related email or text message communications from the vendor or a third party?



[411] *See* Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5)(B).

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

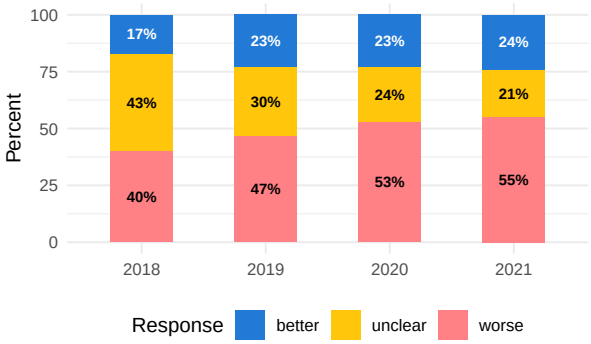
[413] *See* The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(d).

Traditional Ads

The Traditional or Contextual Advertisements evaluation question indicates whether advertisements are displayed to any users without using any collected personal information from the product. Traditional advertisements (otherwise referred to as contextual advertisements) display products and services to users based only on the relevant content or web page 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 profile audience that may be more relevant to users than simply contextual advertisements.

A "better" response to this evaluation question indicates the product does not display any traditional or contextual ads on the product. This question is also included in our basic evaluation process.[414,415]

Figure 184: Traditional Ads: 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?

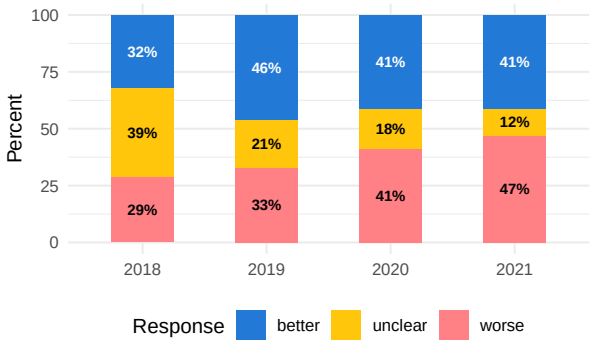


Behavioral Ads

The Behavioral Advertising evaluation question indicates whether advertisements are displayed to any users based on collected personal information or behavioral information on how users use the product. Behavioral advertisements take targeted advertisements one step further, collecting 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 specific information they received from the user's activities on the product.

A "better" response to this evaluation question indicates the product does not display any targeted or behavioral ads on the product. This question is also included in our basic evaluation process.[416,417,418]

Figure 185: Behavioral Ads: Do the policies clearly indicate whether or not behavioral advertising based on a user's personal information are displayed?



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

[415] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(a), (e)(1), (e)(4), (t).

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

[417] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(6), (ah).

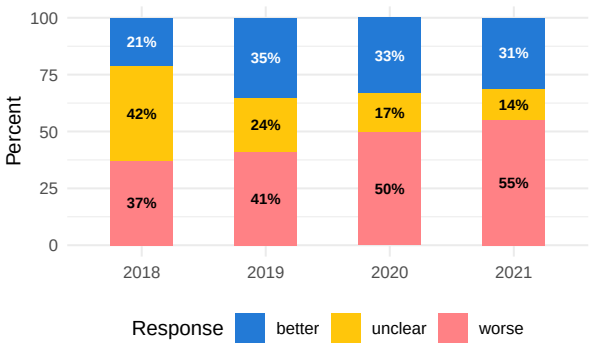
[418] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).

Third-Party Tracking

The Third-PartyTracking evaluation question indicates whether the company allows third-party companies to use cookies or other tracking technologies on its product, which enables those third parties companies to collect and use a user's personal information for their own purposes. A company should not permit third-party advertising services or tracking technologies to collect any information from a user while using the service. A user's personal information provided to a product should not be also used by a third party to persistently track that user's behavioral actions on the product to influence what content they see in the product and elsewhere online. Third-party tracking can influence a user's decision-making processes without their knowledge, which may cause unintended harm.

A "better" response to this evaluation question indicates the company does not allow third-party companies to use cookies or other tracking technologies on its product. This question is also included in our basic evaluation process.[419,420,421]

Figure 186: Third-Party Tracking: Do the policies clearly indicate whether or not third-party advertising services or tracking technologies collect any information from a user of the product?



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

[420] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(7).

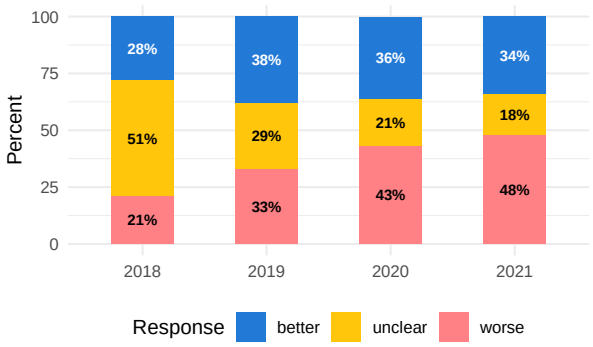
[421] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(k), (l), (ah), (aj).

Track Users

The Track Users evaluation question indicates that the product allows a third-party company to use cookies or other tracking technologies on its service for the specific purpose of allowing third-party companies to display advertisements to the service's users on other apps and services across the internet. A company should not track users to target them with advertisements on other third-party websites or services. A user's personal information provided to a product should not be used by a third party to persistently track that user's behavioral actions over time and across the internet on other apps and services.

A "better" response to this evaluation question indicates the company does not allow third-party companies to track users over time and across the internet on other apps and services. This question is also included in our basic evaluation process.[422,423,424,425,426]

Figure 187: Track Users: 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?



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

[423] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1.

[424] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(B).

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

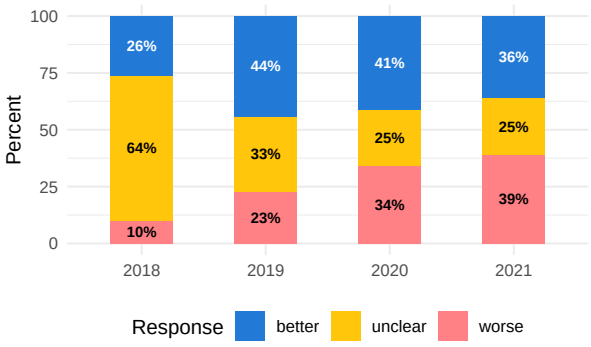
[426] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(e)(4), (k), (ah), (aj).

Data Profile

The Data Profile evaluation question indicates that a product allows third-party companies to use cookies or other tracking technologies on the product, which enables those third-party companies to create a behavioral profile about a user based on the user's personal information for advertising or marketing purposes across the internet. A company should not allow third parties to use a user's data to create a profile, engage in data enhancement or social advertising, or target advertising based on that profile. 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.

A "better" response to this evaluation question indicates the company does not allow third-party companies to create a behavioral profile about a user based on the user's personal information for advertising or marketing purposes. This question is also included in our basic evaluation process.[427,428,429,430,431,432]

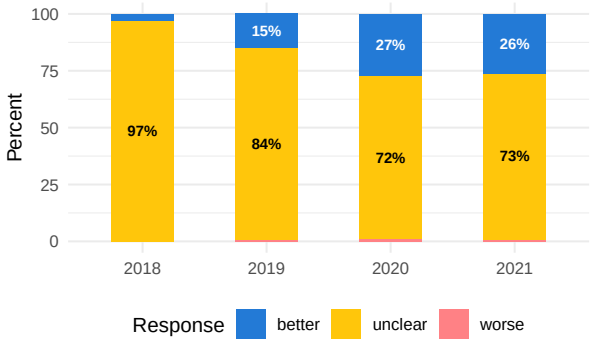
Figure 188: Data Profile: Do the policies clearly indicate whether or not the vendor allows third parties to use a student's data to create an automated profile, engage in data enhancement, conduct social advertising, or target advertising to students, parents, teachers, or the school?



Filter Ads

The Filter Ads evaluation question indicates that age-inappropriate advertisements (e.g., alcohol, smoking, gambling, violence, or sexual content) are excluded from the product if used by children or students. A child's personal information provided to a product should not be used to exploit that user's specific knowledge, traits, and viewing behaviors to influence their desire to purchase goods and services that are inappropriate for minors. A "better" response to this evaluation question indicates age-inappropriate advertisements are excluded from the product if used by children or students.[433,434]

Figure 189: Filter Ads: Do the policies clearly indicate whether or not the vendor or third party filters inappropriate advertisements (e.g., alcohol, gambling, violence, or sexual content)?



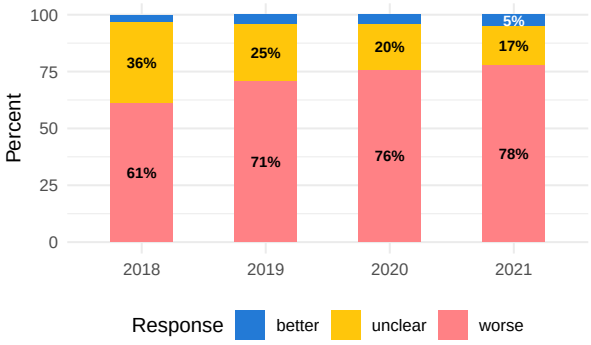
[427] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[428] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(2), 22584(e)(2).
[429] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.
[430] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(e)(4), (v)(1)(K), (z), (aj).
[431] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.
[432] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(4)(E)(i), 2584(b)(4)(E)(ii).

[433] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.
[434] *See* Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5)(B).

Marketing Messages

The Marketing Messages evaluation question indicates the company sends first-party marketing emails, text messages, or other related communications to its users for advertising purposes. A company should not send first-party marketing messages to children or students. Any marketing communications should only be sent to adult users of the product if separate opt-in consent was obtained for that purpose. A "better" response to this evaluation question indicates the company does not send first-party marketing emails, text messages, or other related communications to its users for advertising purposes.[435,436,437,438]

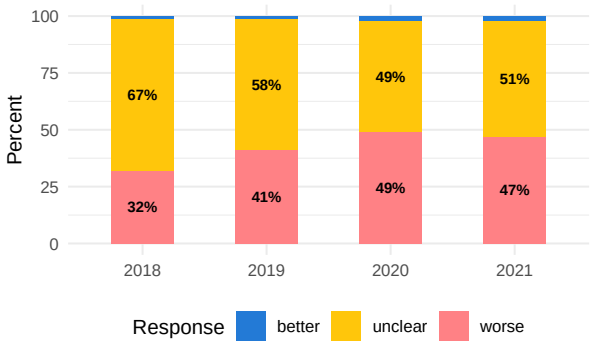
Figure 190: Marketing Messages: Do the policies clearly indicate whether or not the vendor may send marketing emails, text messages, or other related communications that may be of interest to a user?



Third-Party Promotions

The Third-Party Promotions evaluation question indicates that the company may send its own first-party or third-party promotional sweepstakes, contests, or surveys to users of the product. A company should not encourage the submission of personal information with the use of promotions, prizes, or games. A "better" response to this evaluation question indicates the company does not send its own first-party or third-party promotional sweepstakes, contests, or surveys to users of the product.[439,440,441,442]

Figure 191: Third-Party Promotions: 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?



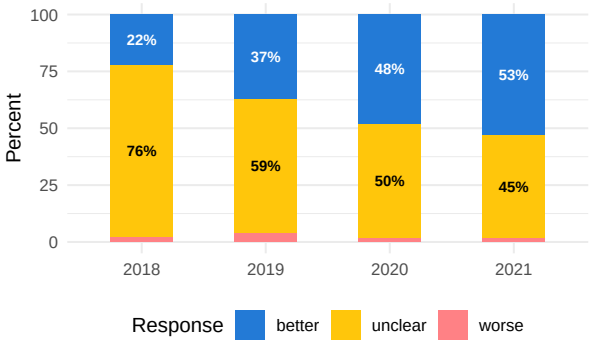
[435] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.7.
[436] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.
[437] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).
[438] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(t).

[439] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.7.
[440] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(d).
[441] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(A).
[442] *See* Protection of Pupil Rights Act (PPRA), 34 C.F.R. § 98.3.

Unsubscribe Ads

The Unsubscribe Ads evaluation question indicates that the company provides users with the ability to opt out from first-party or third-party advertising on the product. A company should provide privacy controls for users to easily opt out of behavioral or targeted advertising to users based on their personal information. A "better" response to this evaluation question indicates the company does provide users with the ability to opt out from first-party or third-party advertising on the product.[443,444]

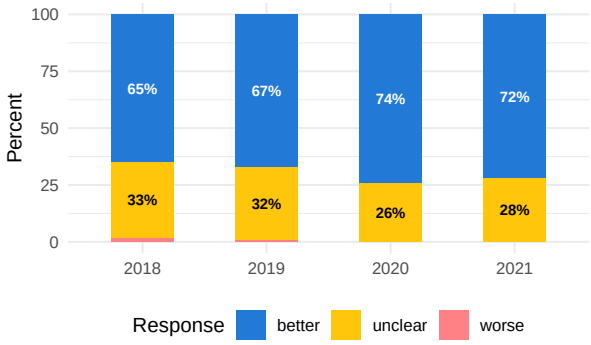
Figure 192: Unsubscribe Ads: Do the policies clearly indicate whether or not a user can opt out of traditional, contextual, or behavioral advertising?



Unsubscribe Marketing

The Unsubscribe Marketing evaluation question indicates that the company provides users with the ability to opt out from first-party or third-party marketing communications. A company should provide privacy controls for users to easily opt in or opt out of different marketing uses of their personal information. A "better" response to this evaluation question indicates the company does provide users with the ability to opt out from first-party or third-party marketing communications.[445,446]

Figure 193: Unsubscribe Marketing: Do the policies clearly indicate whether or not a user can opt out or unsubscribe from a vendor or third party marketing communication?



[443] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(a)(2).

[444] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(7).

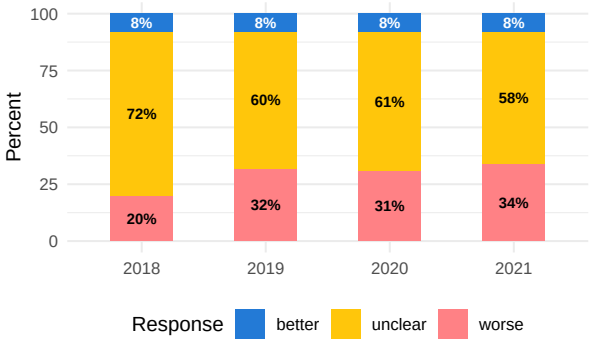
[445] *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 16 C.F.R. Part 316.5.

[446] *See* General Data Protection Regulation (GDPR), Automated individual decision-making, including profiling, Art. 21(2), 21(3).

DoNotTrack Response

The DoNotTrack Response evaluation question indicates whether the product responds to a user's browser-based DoNotTrack signal that provides notice to the company that the user requests to exercise their right to opt out of third-party tracking on the product. A "better" response to this evaluation question indicates the product does respond to a user's browser-based DoNotTrack signal.[447]

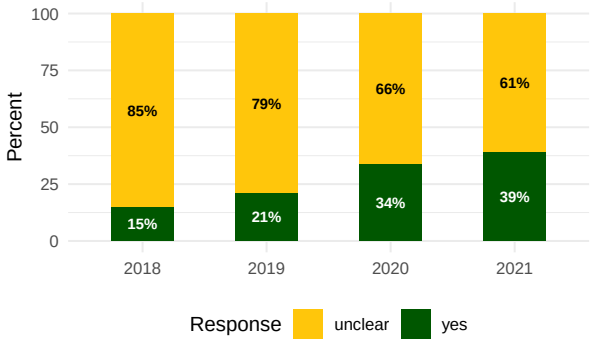
Figure 194: DoNotTrack Response: Do the policies clearly indicate whether or not the vendor responds to a "Do Not Track" signal or other opt-out mechanisms from a user?



DoNotTrack Description

The DoNotTrack Description evaluation question indicates that a hyperlink is available in the product's privacy policy to a location containing an alternative opt-out method not to be tracked by the product. This evaluation question does not have a "better" or "worse" qualitative component.[448]

Figure 195: DoNotTrack Description: Do the policies clearly indicate whether the vendor provides a link to a description and the effects of any program or protocol the vendor follows that offers consumers a choice not to be tracked?



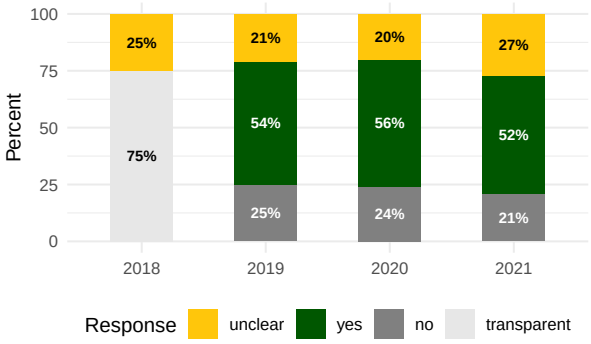
[447] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(5).

[448] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(7).

Actual Knowledge

The Actual Knowledge evaluation question indicates that the company has actual knowledge that users of the product are under the age of 13 because the product utilizes an age-gate or a user's birthday is collected upon account registration in the product. If a company has actual knowledge that a user is under the age of 13, then the product should apply additional privacy protections to children using the product. This evaluation question does not have a "better" or "worse" qualitative component.[449],[450]

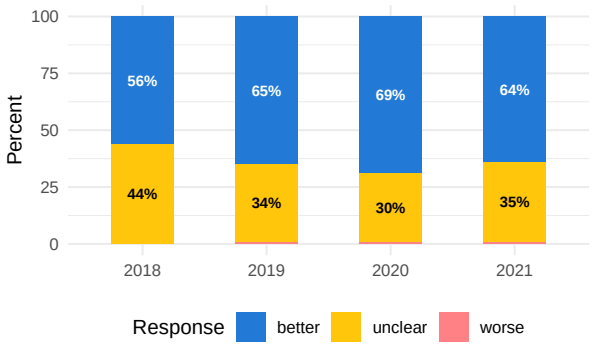
Figure 196: Actual Knowledge: Do the policies clearly indicate whether or not the vendor has actual knowledge that personal information from children under 13 years of age is collected by the product?



COPPA Notice

The Children's Online Privacy Protection Act (COPPA) Notice evaluation question indicates that children's privacy is applicable to the product because children are an intended audience. A company should provide a separate section or separate children's privacy statement that specifies the different data collection, use, and disclosure practices that apply to children using the product. A "better" response to this evaluation question indicates that children's privacy is applicable to the product because children are an intended audience.[451]

Figure 197: COPPA Notice: Do the policies clearly indicate whether or not the vendor describes: (1) what information is collected from children under 13 years of age, (2) how that information is used, and (3) its disclosure practices for that information?



[449] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Parts 312.2, 312.3(d).

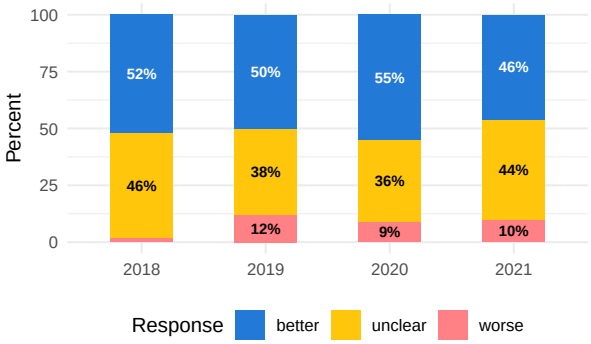
[450] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.120(c)-(d).

[451] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(a); *See also* 16 C.F.R. Part 312.4(d), 312.4(d)(2).

Restrict Account

The Restrict Account evaluation question indicates that the product provides restrictions for the account creation of children under 13 years of age through use of an age-gate or collection of a user's birthday upon account registration. A company should restrict account creation by children to ensure parents register accounts for themselves and their children. Account restriction allows parents to create a child profile which may provide better privacy-protecting data collection and use practices to users who use the managed account or profile. A "better" response to this evaluation question indicates the product does provide restrictions for the account creation of children under 13 years of age.[452]

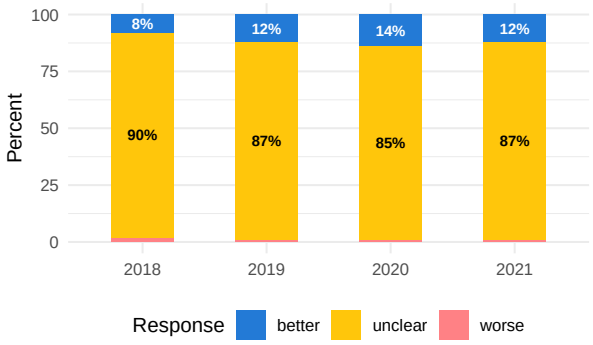
Figure 198: Restrict Account: Do the policies clearly indicate whether or not the vendor prohibits creating an account for a child under 13 years of age?



Restrict Purchase

The Restrict Purchase evaluation question indicates that the product provides restrictions for the purchase of any in-app content or subscriptions for children under 13 years of age through use of an age-gate password or PIN password when a child profile or account is in use. A "better" response to this evaluation question indicates the product does provide restrictions for the purchase of any in-app content or subscriptions for children under 13 years of age.

Figure 199: Restrict Purchase: Do the policies clearly indicate whether or not the vendor restricts in-app purchases for a child under 13 years of age?

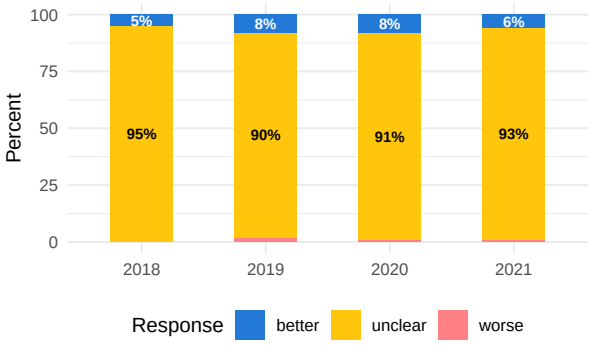


[452] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(b); *See also* 16 C.F.R. Part 312.5(a).

Safe Harbor

The Safe Harbor evaluation question indicates whether the company participates in a safe harbor compliance program. A company may satisfy its obligations under COPPA for children under the age of 13 using the product by participating in a safe harbor program, which is a self-regulatory framework developed by industry groups and approved by the FTC. A "better" response to this evaluation question indicates the company participates in a safe harbor compliance program.[453]

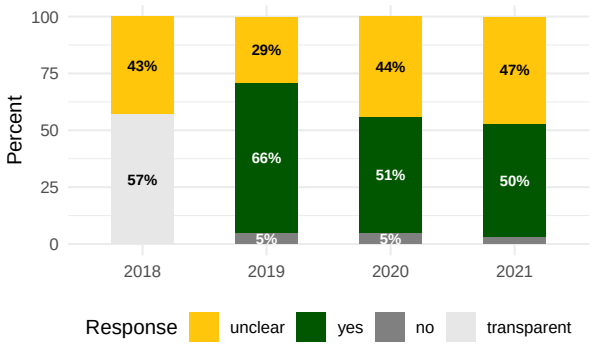
Figure 200: Safe Harbor: Do the policies clearly indicate whether or not the product participates in an FTC-approved COPPA safe harbor program?



School Purpose

The school purpose evaluation question indicates whether the product is primarily designed, marketed, and used for preschool or K-12 school purposes. A company should disclose whether the product is intended to be used in K-12 schools or districts because additional student data privacy laws apply to personal information collected from students. This evaluation question does not have a "better" or "worse" qualitative component. This question is also included in our basic evaluation process.[454,455,456]

Figure 201: School Purpose: Do the policies clearly indicate whether or not the product is primarily used, designed, and marketed for preschool or K-12 school purposes?



[453] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(3); *See also* 16 C.F.R. Part 312.11.

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

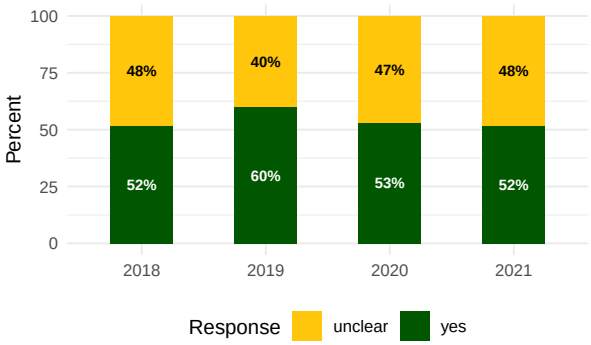
[455] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(m).

[456] *See* Early Learning Personal Information Protection Act (ELPIPA), Cal. B.&P. Code § 22586(a)(1).

Education Records

The Education Records evaluation question indicates whether the product allows the collection of data from students to become protected educational records as part of an educational school or district program. This evaluation question does not have a "better" or "worse" qualitative component.[457,458]

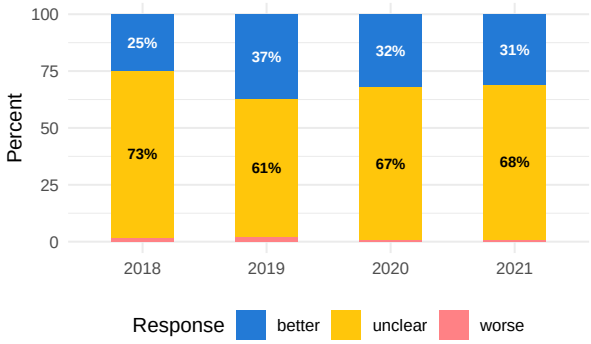
Figure 202: Education Records: Do the policies clearly indicate the process by which education records are entered into the product? For example, are data entered by district staff, school employees, parents, teachers, students, or some other person?



School Contract

The School Contract evaluation question indicates that the company provides a contract or student data privacy agreement to a local education agency to protect student data on the product. A company should put in place additional student data privacy protections that are not disclosed in the privacy policy in contractual agreements with schools and districts to ensure student's data is collected and used only for educational purposes. A "better" response to this evaluation question indicates the company provides a contract or student data privacy agreement to a local education agency to protect student data.[459,460,461]

Figure 203: School Contract: 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?



[457] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1, 99.3.

[458] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(v)(1)(J).

[459] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.7(a).

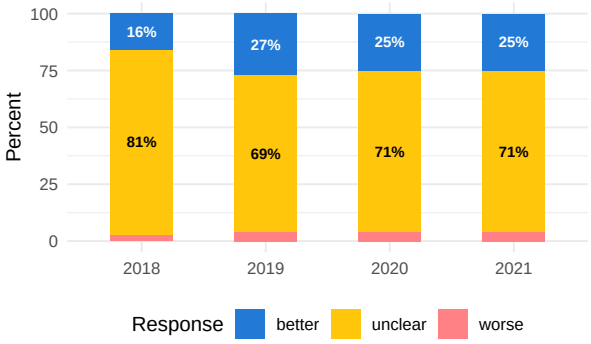
[460] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1.

[461] General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art. 13(2)(e).

School Official

The School Official evaluation question indicates the company does operate under the direct control of any educational institution in which it has entered into a contractual agreement with and is designated a School Official under FERPA. A "better" response to this evaluation question indicates the company does operate under the direct control of any educational institution in which it has entered into a contractual agreement with and is designated a School Official.[462,463,464]

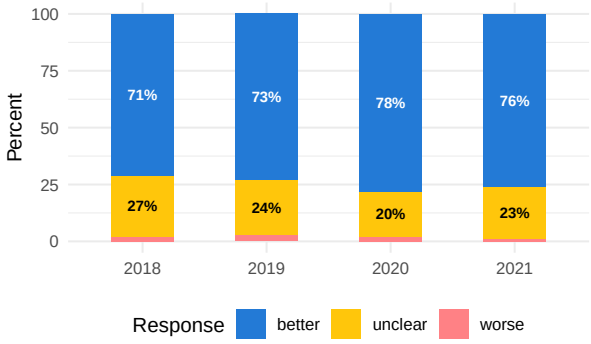
Figure 204: School Official: Do the policies clearly indicate whether or not the vendor is under the direct control of the educational institution and designates themselves a 'School Official' under FERPA?



Parental Consent

The Parental Consent evaluation question indicates that the company obtains verifiable parental consent before they collect, use, or disclose any child or student's personal information. A company should disclose how information is collected from children and how that information is used in order to obtain informed parental consent, because there is an increased risk if a child's personal information is used for unintended purposes. A "better" response to this evaluation question indicates the company obtains verifiable parental consent. This question is also included in our basic evaluation process.[465,466,467]

Figure 205: Parental Consent: Do the policies clearly indicate whether or not the vendor or third party obtains verifiable parental consent before they collect or disclose personal information?



[462] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.7(a).

[463] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(A)-(B), 99.31(a)(1)(ii).

[464] *See* California Privacy of Pupil Records, Cal. Ed. Code §49073.1(b)(8).

[465] *See* 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 also* 15 U.S.C. § 6501(9).

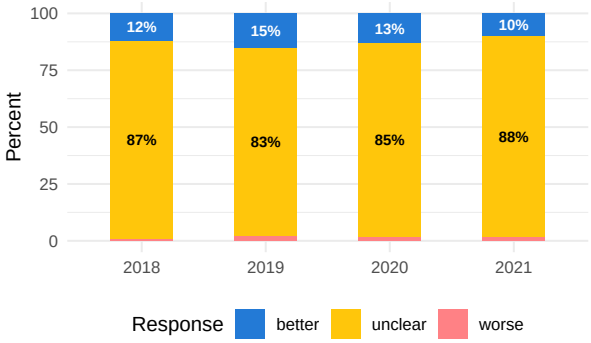
[466] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

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

Limit Consent

The Limit Consent evaluation question indicates that parental consent is obtained for the collection and use of their child's or student's personal information with the product and consent is separate from any additional consent required for the disclosure of their child or student's information to third parties. A company should obtain parental consent for each particular purpose in which personal information is collected and used from children and obtain separate consent for any different purpose, such as disclosing a child's information to third parties for their own purposes. A "better" response to this evaluation question indicates the company obtains additional consent for the disclosure of their child or student's information to third parties.[468]

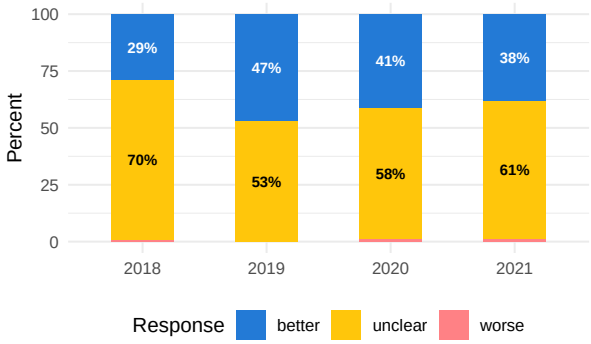
Figure 206: Limit Consent: Do the policies clearly indicate whether or not a parent can consent to the collection and use of their child's personal information without also consenting to the disclosure of the information to third parties?



Withdraw Consent

The Withdraw Consent evaluation question indicates that the company will prevent further collection and use of a child's personal information if requested from a parent or guardian. A company should respond to a verifiable request from a parent or guardian to opt out from the collection, use, or disclosure of their child's or student's personal information. A "better" response to this evaluation question indicates the company will prevent further collection and use of a child's personal information if requested from a parent or guardian.[469]

Figure 207: Withdraw Consent: Do the policies clearly indicate whether or not the vendor responds to a request from a parent or guardian to prevent further collection of their child's information?



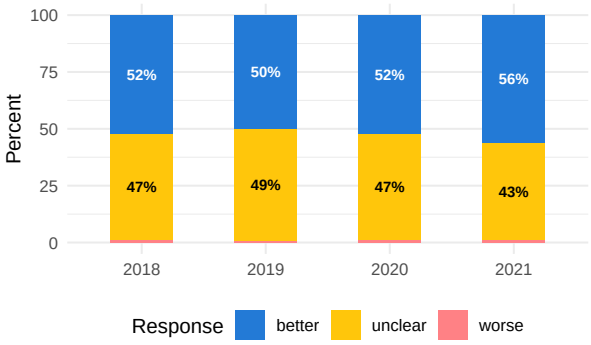
[468] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(a)(2).

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

Delete Child-PII

The Delete Child-PII evaluation question indicates that the company will delete personal information from a child or student under 13 years of age if the information is collected without parental consent. A company should respond to any requests to delete personal information from the product if they receive a verifiable request that the information is from a particular user who is under the age of 13 and was collected without parental consent. A "better" response to this evaluation question indicates the company will delete personal information from a child or student under 13 years of age if the information is collected without parental consent.[470,471,472]

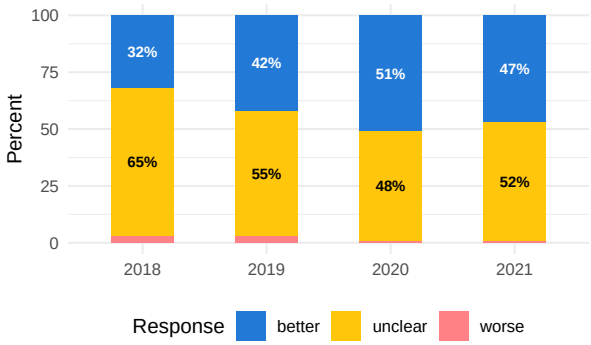
Figure 208: Delete Child-PII: Do the policies clearly indicate whether or not the vendor deletes personal information from a student or child under 13 years of age if collected without parental consent?



Consent Method

The Consent Method evaluation question indicates the company's different methods available for parents or guardians to provide verifiable parental consent for their children's use of the product. A company should disclose to parents how they can provide parental consent such as creating a registered account with the product, creating a separate child profile, or using another COPPA-recognized method such as a consent form signed by the parent, a monetary transaction, a toll-free telephone number or videoconference, or verifying a parent's identity by checking a form of government-issued identification. A "better" response to this evaluation question indicates the company discloses the methods available for parents or guardians to provide verifiable parental consent. This question is also included in our basic evaluation process.[473,474]

Figure 209: Consent Method: 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?



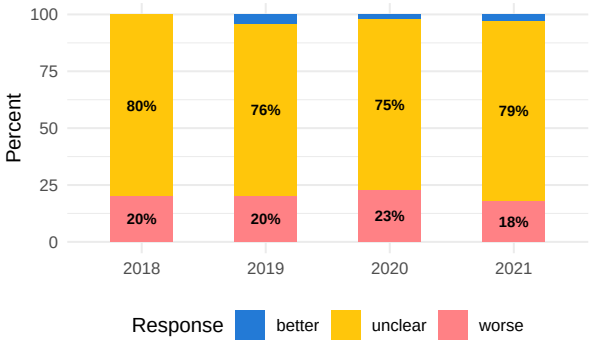
[470] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(1).
[471] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part312.6(c).
[472] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

[473] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(1)-(2)(i)-(vi).
[474] *See* General Data Protection Regulation (GDPR), Conditions Applicable to Child's Consent in Relation to Information Society Services, Art. 8(2).

Internal Operations

The Internal Operations evaluation question indicates whether personal information from children under 13 years of age may be collected without parental consent by the company and shared with third parties for the company's own internal operation purposes. A "better" response to this evaluation question indicates the product does not collect personal information from children under 13 years of age without parental consent.[475,476]

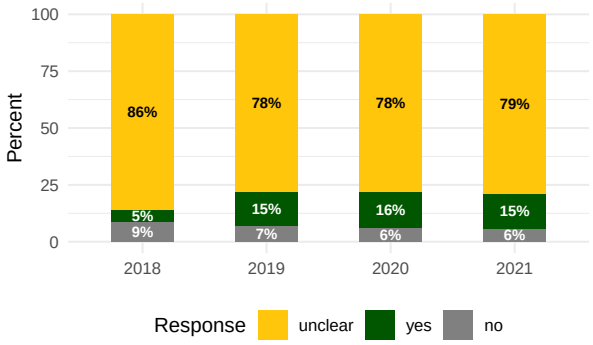
Figure 210: Internal Operations: Do the policies clearly indicate whether or not the vendor can collect and use personal information from children without parental consent to support the 'internal operations' of the vendor's product?



COPPA Exception

The Children's Online Privacy Protection Act (COPPA) Exception evaluation question indicates an exception exists that does not require the company to obtain prior parental consent in order to collect a child's personal information for the sole purpose of contacting a parent and obtaining consent. This evaluation question does not have a "better" or "worse" qualitative component.[477,478,479,480]

Figure 211: COPPA Exception: Do the policies clearly indicate whether or not the vendor collects personal information from children without verifiable parental consent for the sole purpose of trying to obtain consent under COPPA?



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

[476] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(7).

[477] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(1).

[478] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(2).

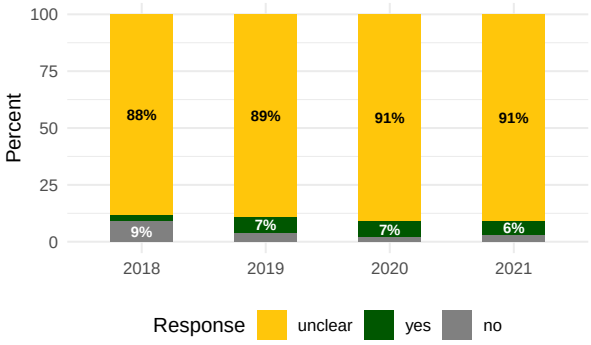
[479] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(3)-(4).

[480] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(7).

FERPA Exception

The Family Educational Rights and Privacy Act (FERPA) Exception evaluation question indicates an exception exists that does not require the company to obtain prior parental consent in order to collect a student's personal information for the sole purpose of sharing with other school officials, including teachers within the same educational institution. This evaluation question does not have a "better" or "worse" qualitative component.[481,482,483,484,485]

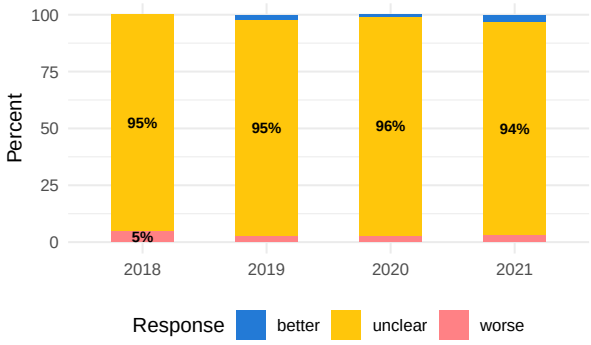
Figure 212: FERPA Exception: Do the policies clearly indicate whether or not the vendor may disclose personal information without verifiable parental consent under a FERPA exception?



Directory Information

The Directory Information evaluation question indicates what type of student information can be disclosed for an educational purpose without parental consent which may include, but is not limited to, the student's name, address, telephone number, email address, photograph, date and place of birth, major field of study, grade level, or enrollment status. A company should provide parents or guardians with the ability to opt out of disclosing their student's personal information as directory information with their school or district. A "better" response to this evaluation question indicates the product does not disclose a student's information for the purposes of directory information without parental consent.[486]

Figure 213: Directory Information: Do the policies clearly indicate whether or not the vendor discloses student information as 'Directory Information' under a FERPA exception?



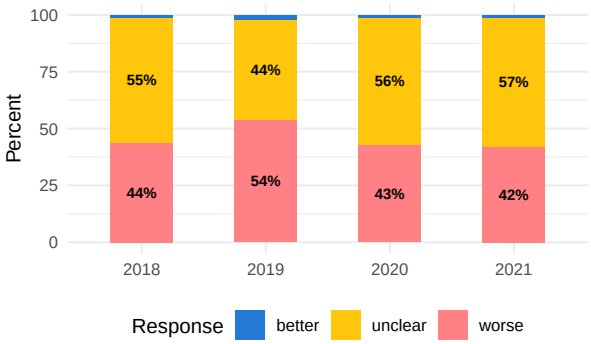
[481] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(A).
[482] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(B).
[483] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(3).
[484] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.31(a)(6), 99.31(b)(2).
[485] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.31(b)(1).

[486] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Parts 99.3, 99.37.

School Consent

The School Consent evaluation question indicates whether the responsibility for obtaining verified parental consent is transferred to the school or district. A company is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from students under 13 years of age. However, COPPA allows schools to act as an intermediary for parental consent in the process of collecting personal information from students, but this consent is limited to the educational context where the product is used, and where students' information is collected solely for the use and educational benefit of the school or district. A "better" response to this evaluation question indicates the company does not transfer the responsibility for obtaining verified parental consent to the school or district.

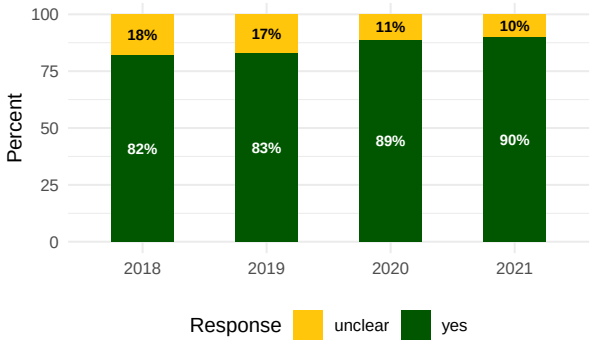
Figure 214: School Consent: Do the policies clearly indicate whether or not responsibility or liability for obtaining verified parental consent is transferred to the school or district?



Policy Jurisdiction

The Policy Jurisdiction evaluation question indicates the domestic state or foreign legal jurisdiction forum that applies to the enforcement of the company's policies. A company should provide a legal jurisdiction forum for the interpretation and enforcement of the policies that would be considered reasonably accessible by the majority of users of the product. This evaluation question does not have a "better" or "worse" qualitative component.

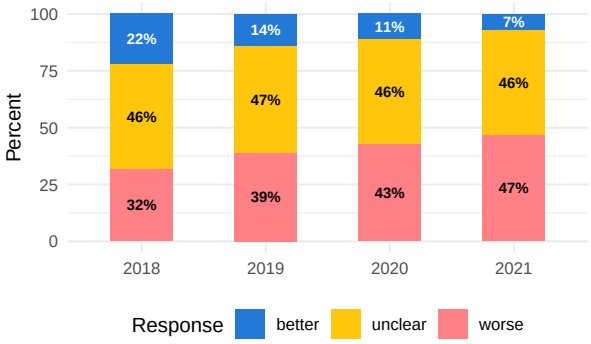
Figure 215: Policy Jurisdiction: Do the policies clearly indicate the vendor's jurisdiction that applies to the construction, interpretation, and enforcement of the policies?



Dispute Resolution

The Dispute Resolution evaluation question indicates the company has a requirement that users must waive the right to a jury trial and settle any disputes by Alternative Dispute Resolution (ADR). A company should provide users with the opportunity to opt-out of the requirement that they must settle any disputes by Alternative Dispute Resolution (ADR) during account registration. A "better" response to this evaluation question indicates the company does not require users to waive the right to a jury trial and settle any disputes by Alternative Dispute Resolution.

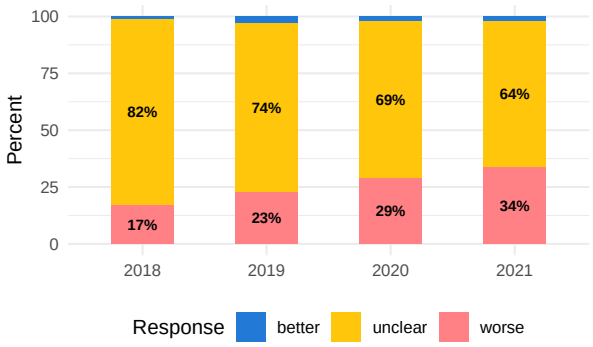
Figure 216: Dispute Resolution: Do the policies clearly indicate whether or not the vendor requires a user to waive the right to a jury trial, or settle any disputes by Alternative Dispute Resolution (ADR)?



Class Waiver

The Class Waiver evaluation question indicates whether the company has a requirement that users must waive any legal rights to join a class-action lawsuit in the event of a dispute. A company should provide users with the opportunity to opt out of the requirement that they waive the right to join a class-action lawsuit during account registration to preserve all their legal rights in the event of a dispute with the company. A "better" response to this evaluation question indicates the company does not require users waive any legal rights to join a class-action lawsuit.

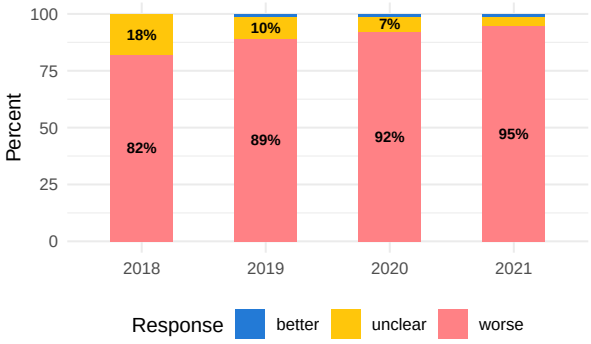
Figure 217: Class Waiver: Do the policies clearly indicate whether or not the vendor requires the user to waive their right to join a class action lawsuit?



Law Enforcement

The Law Enforcement evaluation question indicates that a user's information may be shared with government, private, or legal authorities to protect the company or to protect the health, privacy, or safety of the product's users. A "better" response to this evaluation question indicates the product does not disclose a user's information to government, private, or legal authorities.[487,488,489,490,491]

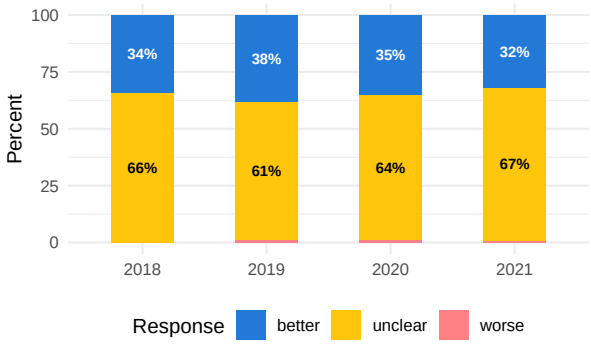
Figure 218: Law Enforcement: Do the policies clearly indicate whether or not the vendor can use or disclose a user's data under a requirement of applicable law to comply with a legal process, to respond to governmental requests, to enforce their own policies, for assistance in fraud detection and prevention, or to protect the rights, privacy, safety or property of the vendor, its users, or others?



Privacy Badge

The Privacy Badge evaluation question indicates that the company has made a commitment to a third-party privacy certification, badge, award, or principles of a privacy pledge. A company that has earned a certification toward their better privacy-protecting practices – and has demonstrated that compliance to its users – can create stronger trust and safety with the users of its product and differentiate themselves from their competitors on privacy. A "better" response to this evaluation question indicates the company has made a commitment to a third-party privacy certification, badge, award, or principles of a privacy pledge.[492]

Figure 219: Privacy Badge: Do the policies clearly indicate whether or not the vendor has signed any privacy pledges or received any other privacy certifications?



[487] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(5)-(6).

[488] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(5),(9),(10),(13)-(16); 34 C.F.R. Part 99.36.

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

[490] *See* California Electronic Communications Privacy Act, Cal. Pen. Code § 1546-1546.4.

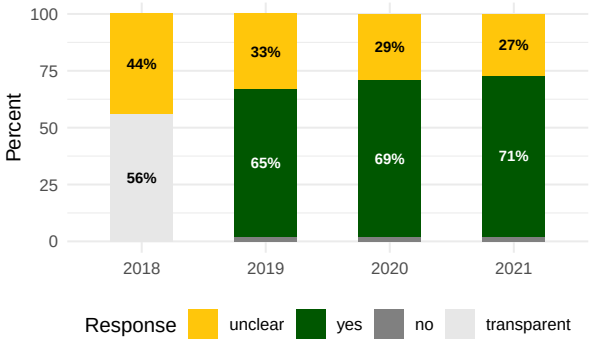
[491] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.145(a)(1)-(5).

[492] *See* General Data Protection Regulation (GDPR), Responsibility of the Controller, Art. 24(3).

GDPR Jurisdiction

The General Data Protection Regulation (GDPR) evaluation question indicates that the company has users located in Europe and is subject to international data privacy jurisdiction laws. A company with users in other countries should disclose how its data practices are applied to different countries and have suitable safeguards in place relating to the transfer of users' data between countries. This evaluation question does not have a "better" or "worse" qualitative component.[493,494,495,496,497,498,499]

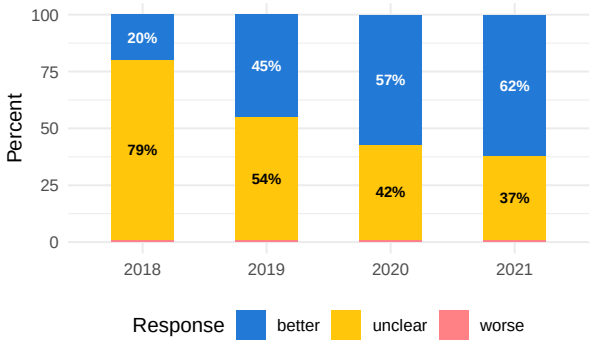
Figure 220: GDPR Jurisdiction: Do the policies clearly indicate whether or not a user's data are subject to International data transfer or jurisdiction laws, such as a privacy shield or a safe harbor framework that protects the cross-border transfer of a user's data?



GDPR Role

The GDPR Role evaluation question indicates whether the company is categorized as a data controller or a data processor, and if a Data Protection Officer (DPO) can be contacted. A company should disclose the type of relationship it has with users of its product as either a controller or processor. A company should also provide information to users on how to contact the company's data protection officer to answer privacy-related questions about the product. A "better" response to this evaluation question indicates the company is either a data controller or a data processor and contact information for a DPO is provided.[500,501,502,503,504,505,506,507]

Figure 221: GDPR Role: Do the policies clearly indicate whether or not the vendor is categorized as a Data Controller or a Data Processor, and whether it has identified a Data Protection Officer (DPO) for the purposes of GDPR compliance?



[493] *See* General Data Protection Regulation (GDPR), Territorial Scope, Art. 3(1), 3(2)(a)-(b), 3(3).
[494] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(20), 4(23)(a)-(b).
[495] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art. 13(1)(f), 14(1)(f).
[496] *See* General Data Protection Regulation (GDPR), Right of access by the data subject, Art. 15(2).
[497] *See* General Data Protection Regulation (GDPR), General principle for transfers, Art. 44.
[498] *See* General Data Protection Regulation (GDPR), Transfers on the basis of an adequacy decision, Art. 45(1).
[499] *See* General Data Protection Regulation (GDPR), Representatives of controllers or processors not established in the Union, Art. 27(1), 27(2), 27(3), 27(4).

[500] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(y).
[501] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(7).
[502] *See* General Data Protection Regulation (GDPR), Records of Processing Activities, Art. 30(1)-(4).
[503] *See* General Data Protection Regulation (GDPR), Material Scope, Art. 2(1).
[504] *See* General Data Protection Regulation (GDPR), Definitions, Art. 4(2), 4(8).
[505] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data are collected from the data subject, Art. 13(1)(b).
[506] *See* General Data Protection Regulation (GDPR), Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(b).
[507] *See* General Data Protection Regulation (GDPR), Designation of the data protection officer, Art. 37(1)(b).

Additional Reading Statistics

Reading Time

Figure 222: Reading Time versus Rating Score.

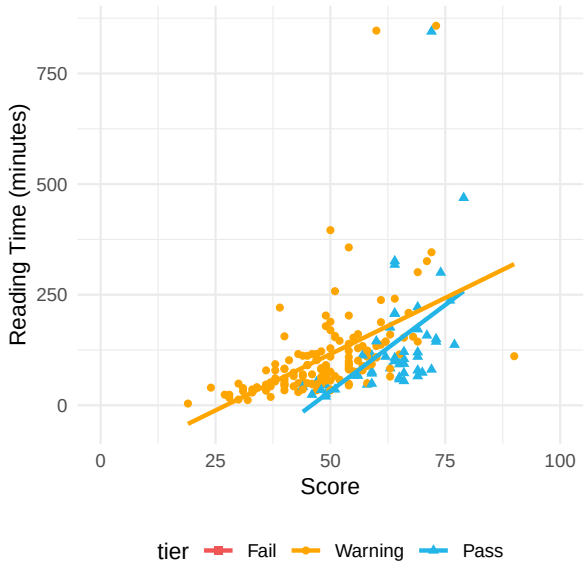
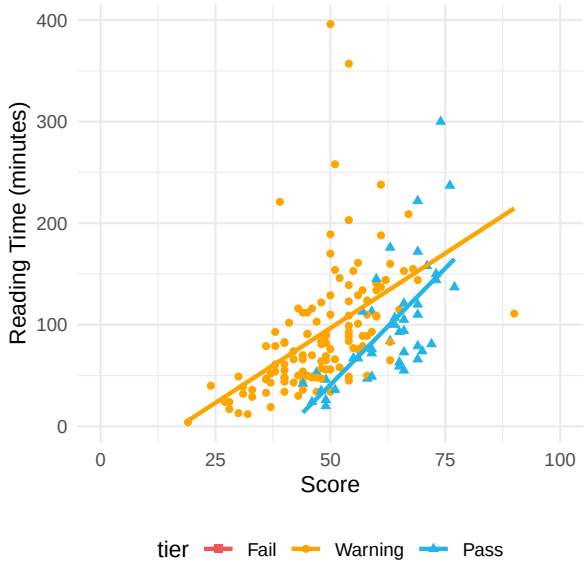


Figure 223: Reading Time versus Rating Score. 'Big Tech' supressed from data.



Flesch-Kincaid Grade Level

Figure 224: Flesch-Kincaid Grade Level versus Rating Score.

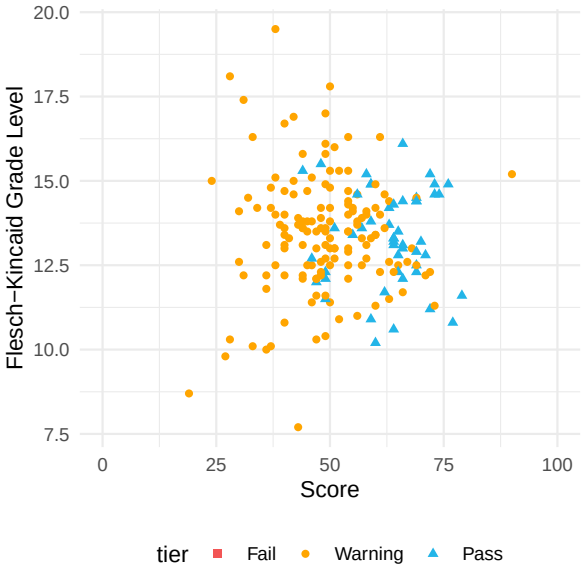


Figure 225: Flesch-Kincaid Grade Level versus score. 'Big Tech' supressed from data.

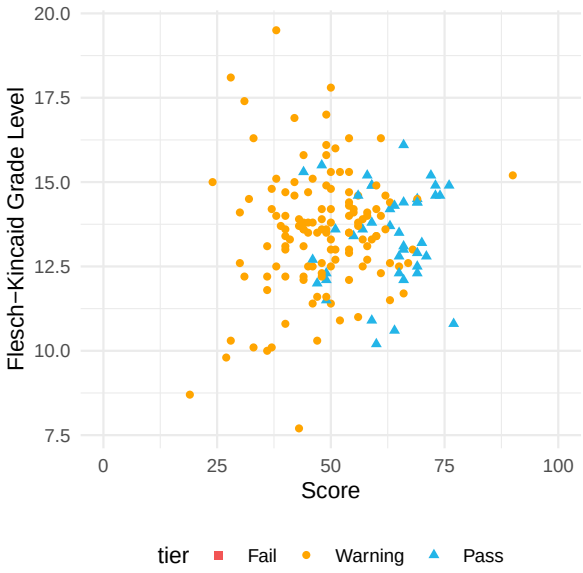
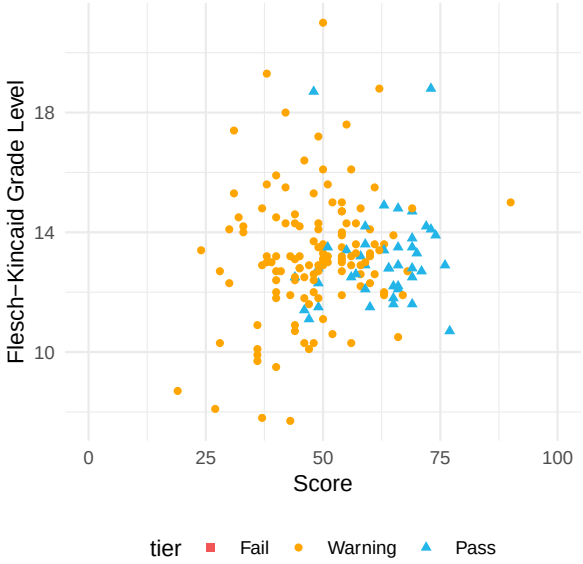


Figure 226: Privacy policy only: Flesch-Kincaid Grade Level versus Rating Score 'Big Tech' supressed from data.



List of Products Evaluated 2021

Product	Evaluation URL	Rating	Basic Score	Full Score
ABCmouse.com	https://privacy.commonsense.org/evaluation/ABCmouse.com	Warning	79	69
ABCya	https://privacy.commonsense.org/evaluation/ABCya	Warning	56	49
Academic Earth	https://privacy.commonsense.org/evaluation/Academic-Earth	Warning	43	38
Accelify	https://privacy.commonsense.org/evaluation/accelify	Warning	41	31
Achieve3000 Literacy Solutions	https://privacy.commonsense.org/evaluation/achieve3000-literacy-solutions	Pass	96	66
Actively Learn	https://privacy.commonsense.org/evaluation/actively-learn	Warning	72	50
Adobe Spark EDU	https://privacy.commonsense.org/evaluation/Adobe-Spark-EDU	Pass	90	66
Akindi	https://privacy.commonsense.org/evaluation/akindi	Warning	37	28
Alison	https://privacy.commonsense.org/evaluation/Alison	Warning	53	48
Amazon Alexa	https://privacy.commonsense.org/evaluation/Amazon-Alexa	Warning	53	49
Amazon Kids+	https://privacy.commonsense.org/evaluation/Amazon-Kids	Warning	60	47
Amazon Kindle	https://privacy.commonsense.org/evaluation/Amazon-Kindle	Warning	62	54
Amazon Prime Video	https://privacy.commonsense.org/evaluation/Amazon-Prime-Video	Warning	60	47
Angry Birds	https://privacy.commonsense.org/evaluation/angry-birds	Warning	57	46
Animal Jam	https://privacy.commonsense.org/evaluation/Animal-Jam	Warning	49	40
Animoto	https://privacy.commonsense.org/evaluation/animoto	Warning	71	61
Apollo	https://privacy.commonsense.org/evaluation/apollo	Warning	25	24
Apple School Manager	https://privacy.commonsense.org/evaluation/Apple-School-Manager	Pass	79	64
Apple Siri	https://privacy.commonsense.org/evaluation/Apple-Siri	Pass	79	64
AppleTV+	https://privacy.commonsense.org/evaluation/AppleTV	Pass	79	64
Bark	https://privacy.commonsense.org/evaluation/Bark	Warning	82	66
Big History Project	https://privacy.commonsense.org/evaluation/Big-History-Project	Warning	87	63
Blackboard	https://privacy.commonsense.org/evaluation/Blackboard	Warning	78	67
Bloomz	https://privacy.commonsense.org/evaluation/bloomz	Warning	69	52
BrainPOP	https://privacy.commonsense.org/evaluation/brainpop	Warning	76	63
Brainquake	https://privacy.commonsense.org/evaluation/brainquake	Warning	47	43
Branching Minds	https://privacy.commonsense.org/evaluation/Branching-Minds	Pass	84	51
Brightspace	https://privacy.commonsense.org/evaluation/Brightspace	Warning	76	57
Buzzmath	https://privacy.commonsense.org/evaluation/Buzzmath	Warning	63	44
Calm	https://privacy.commonsense.org/evaluation/Calm	Warning	41	42
Canva - Graphic Design & Video	https://privacy.commonsense.org/evaluation/Canva—Graphic-Design–Video	Warning	68	56
Canvas	https://privacy.commonsense.org/evaluation/canvas	Warning	63	46
Capit	https://privacy.commonsense.org/evaluation/capit	Pass	79	66

Cisco Webex	https://privacy.commonsense.org/evaluation/Cisco-Webex	Warning	71	59
Class Charts	https://privacy.commonsense.org/evaluation/class-charts	Warning	49	37
Class Hub	https://privacy.commonsense.org/evaluation/Class-Hub	Pass	66	48
Class123	https://privacy.commonsense.org/evaluation/class123	Warning	35	33
Classcraft	https://privacy.commonsense.org/evaluation/Classcraft	Warning	69	54
ClassDojo	https://privacy.commonsense.org/evaluation/classdojo	Pass	90	74
ClassFlow	https://privacy.commonsense.org/evaluation/classflow	Pass	87	69
Classkick	https://privacy.commonsense.org/evaluation/classkick	Pass	93	69
ClassMarker	https://privacy.commonsense.org/evaluation/ClassMarker	Warning	47	44
Clever	https://privacy.commonsense.org/evaluation/Clever	Pass	91	69
Code Combat	https://privacy.commonsense.org/evaluation/code-combat	Warning	60	42
Code.org	https://privacy.commonsense.org/evaluation/code.org	Pass	96	77
Codecademy: Code Hour	https://privacy.commonsense.org/evaluation/codecademy:-code-hour	Warning	66	46
CodeHS	https://privacy.commonsense.org/evaluation/codehs	Warning	63	48
Coolmath	https://privacy.commonsense.org/evaluation/Coolmath	Warning	34	27
Curious World - Early learning games, videos and books for kids	https://privacy.commonsense.org/evaluation/curious-world—early-learning-games,-videos-and-books-for-kids	Warning	40	38
Curriki	https://privacy.commonsense.org/evaluation/Curriki	Pass	75	69
Dailymotion	https://privacy.commonsense.org/evaluation/Dailymotion	Warning	60	54
Desmos	https://privacy.commonsense.org/evaluation/desmos	Pass	87	69
Dictionary.com	https://privacy.commonsense.org/evaluation/dictionary.com	Warning	57	54
Discord - Talk, Chat & Hangout	https://privacy.commonsense.org/evaluation/Discord—Talk-Chat–Hangout	Warning	51	40
Discovery+	https://privacy.commonsense.org/evaluation/Discovery	Warning	54	50
Disney+	https://privacy.commonsense.org/evaluation/Disney	Warning	68	61
DreamBox Learning Math	https://privacy.commonsense.org/evaluation/DreamBox-Learning-Math	Pass	90	59
Dropbox	https://privacy.commonsense.org/evaluation/Dropbox	Warning	54	47
Duolingo	https://privacy.commonsense.org/evaluation/duolingo	Warning	57	48
Duolingo ABC - Learn to Read	https://privacy.commonsense.org/evaluation/Duolingo-ABC—Learn-to-Read	Pass	85	65
e-hallpass	https://privacy.commonsense.org/evaluation/e-hallpass	Warning	56	37
EasyBib	https://privacy.commonsense.org/evaluation/easybib	Warning	56	50
eBay	https://privacy.commonsense.org/evaluation/eBay	Warning	57	51
Edgenuity	https://privacy.commonsense.org/evaluation/Edgenuity	Warning	62	44
Edmodo	https://privacy.commonsense.org/evaluation/edmodo	Warning	69	58
eDoctrina	https://privacy.commonsense.org/evaluation/eDoctrina	Warning	56	32
EDpuzzle	https://privacy.commonsense.org/evaluation/edpuzzle	Pass	91	73
Edsby	https://privacy.commonsense.org/evaluation/edsby	Pass	87	55

Edthena	https://privacy.commonsense.org/evaluation/edthena	Pass	81	64
Educreations Interactive Whiteboard	https://privacy.commonsense.org/evaluation/educreations-interactive-whiteboard	Warning	56	44
Edulastic	https://privacy.commonsense.org/evaluation/edulastic	Pass	94	59
edWeb	https://privacy.commonsense.org/evaluation/edweb	Warning	68	47
Engrade	https://privacy.commonsense.org/evaluation/Engrade	Warning	62	60
EvaluationKIT	https://privacy.commonsense.org/evaluation/evaluationkit	Warning	54	48
Evernote	https://privacy.commonsense.org/evaluation/evernote	Warning	68	61
Explain Everything	https://privacy.commonsense.org/evaluation/explain-everything	Pass	88	72
ExploreLearning Gizmos	https://privacy.commonsense.org/evaluation/explorelearning-gizmos	Warning	56	45
FaceApp: AI Face Editor	https://privacy.commonsense.org/evaluation/FaceApp-AI-Face-Editor	Warning	57	49
Facebook	https://privacy.commonsense.org/evaluation/Facebook	Warning	47	47
Fitbit	https://privacy.commonsense.org/evaluation/Fitbit	Warning	63	60
Flipgrid	https://privacy.commonsense.org/evaluation/Flipgrid	Pass	82	60
Flocabulary	https://privacy.commonsense.org/evaluation/flocabulary	Pass	93	70
Formative	https://privacy.commonsense.org/evaluation/formative	Pass	93	66
FreshGrade	https://privacy.commonsense.org/evaluation/freshgrade	Pass	90	66
Gaggle	https://privacy.commonsense.org/evaluation/gaggle	Pass	78	56
Garmin Vivofit Jr.	https://privacy.commonsense.org/evaluation/Garmin-Vivofit-Jr.	Warning	46	48
Geoboard, by The Math Learning Center	https://privacy.commonsense.org/evaluation/geoboard,-by-the-math-learning-center	Warning	71	54
GitHub	https://privacy.commonsense.org/evaluation/GitHub	Pass	75	62
GizmoHub	https://privacy.commonsense.org/evaluation/GizmoHub	Warning	71	58
Global Grid for Learning	https://privacy.commonsense.org/evaluation/Global-Grid-for-Learning	Pass	79	49
Goodreads	https://privacy.commonsense.org/evaluation/goodreads	Warning	50	34
Google Assistant	https://privacy.commonsense.org/evaluation/Google-Assistant	Warning	75	71
Google Classroom	https://privacy.commonsense.org/evaluation/Google-Classroom	Pass	88	79
Google Family Link	https://privacy.commonsense.org/evaluation/Google-Family-Link	Warning	75	72
HBO Max	https://privacy.commonsense.org/evaluation/HBO-Max	Warning	63	56
HTC Vive	https://privacy.commonsense.org/evaluation/HTC-Vive	Warning	57	51
Hulu	https://privacy.commonsense.org/evaluation/Hulu	Warning	53	45
i-Ready	https://privacy.commonsense.org/evaluation/i-ready	Pass	84	58
iMessage	https://privacy.commonsense.org/evaluation/iMessage	Pass	79	64
Instagram	https://privacy.commonsense.org/evaluation/instagram	Warning	57	49
Istation	https://privacy.commonsense.org/evaluation/istation	Warning	51	38
iTooch Music	https://privacy.commonsense.org/evaluation/iTooch-Music	Warning	25	30

iTunes U	https://privacy.commonsense.org/evaluation/iTunes-U	Pass	79	64
IXL	https://privacy.commonsense.org/evaluation/IXL	Warning	72	68
Jitsi Meet	https://privacy.commonsense.org/evaluation/Jitsi-Meet	Warning	49	42
Jumbo	https://privacy.commonsense.org/evaluation/Jumbo	Warning	46	36
Kahoot!	https://privacy.commonsense.org/evaluation/kahoot	Pass	76	64
Kami	https://privacy.commonsense.org/evaluation/kami	Pass	90	65
Khan Academy	https://privacy.commonsense.org/evaluation/khan-academy	Pass	88	71
Kiddom	https://privacy.commonsense.org/evaluation/Kiddom	Pass	84	59
KIDOZ	https://privacy.commonsense.org/evaluation/KIDOZ	Warning	65	56
Kids Vehicles: Dora Ice Cream Truck! Counting Game	https://privacy.commonsense.org/evaluation/Kids-Vehicles-Dora-Ice-Cream-Truck-Counting-Game	Warning	12	19
Knewton	https://privacy.commonsense.org/evaluation/knewton	Warning	54	49
Kodable - Coding for Kids	https://privacy.commonsense.org/evaluation/Kodable—Coding-for-Kids	Warning	49	40
Learning.com	https://privacy.commonsense.org/evaluation/Learning.com	Warning	72	50
LearnZillion	https://privacy.commonsense.org/evaluation/learnzillion	Pass	90	63
Lucid Chart	https://privacy.commonsense.org/evaluation/Lucid-Chart	Warning	75	61
Lynda	https://privacy.commonsense.org/evaluation/lynda	Warning	53	40
Matific	https://privacy.commonsense.org/evaluation/matific	Warning	72	54
Messenger Kids	https://privacy.commonsense.org/evaluation/Messenger-Kids	Warning	68	54
MeWe Network	https://privacy.commonsense.org/evaluation/MeWe-Network	Pass	62	47
Microsoft Office 365 Education	https://privacy.commonsense.org/evaluation/Microsoft-Office-365-Education	Pass	88	72
Microsoft Teams	https://privacy.commonsense.org/evaluation/Microsoft-Teams	Warning	79	73
MobyMax	https://privacy.commonsense.org/evaluation/MobyMax	Warning	56	40
Moodle	https://privacy.commonsense.org/evaluation/Moodle	Warning	46	31
Nearpod	https://privacy.commonsense.org/evaluation/nearpod	Warning	88	65
Neo	https://privacy.commonsense.org/evaluation/Neo	Warning	51	36
Netflix	https://privacy.commonsense.org/evaluation/Netflix	Warning	46	40
Newsela	https://privacy.commonsense.org/evaluation/newsela	Warning	74	58
Nitro Type	https://privacy.commonsense.org/evaluation/nitro-type	Warning	41	33
NOGGIN - Preschool shows and educational videos for kids	https://privacy.commonsense.org/evaluation/NOGGIN—Preschool-shows-and-educational-videos-for-kids	Warning	62	49
NoRedInk	https://privacy.commonsense.org/evaluation/noredink	Warning	93	90
NVIDIA	https://privacy.commonsense.org/evaluation/NVIDIA	Warning	43	36
Oculus for Facebook	https://privacy.commonsense.org/evaluation/Oculus-for-Facebook	Warning	50	49
Osmo Numbers	https://privacy.commonsense.org/evaluation/Osmo-Numbers	Warning	71	55
Paramount+	https://privacy.commonsense.org/evaluation/Paramount	Warning	65	54
Parler	https://privacy.commonsense.org/evaluation/Parler	Warning	43	40

Pathway to Financial Success in Schools	https://privacy.commonsense.org/evaluation/Pathway-to-Financial-Success-in-Schools	Warning	62	55
PBS Kids	https://privacy.commonsense.org/evaluation/PBS-Kids	Pass	84	46
Peacock TV	https://privacy.commonsense.org/evaluation/Peacock-TV	Warning	59	55
Pear Deck	https://privacy.commonsense.org/evaluation/pear-deck	Pass	84	59
Pinterest	https://privacy.commonsense.org/evaluation/Pinterest	Warning	50	49
PlayStation	https://privacy.commonsense.org/evaluation/PlayStation	Warning	62	50
Plickers	https://privacy.commonsense.org/evaluation/plickers	Warning	57	46
Pokémon GO	https://privacy.commonsense.org/evaluation/pokémon-go	Warning	68	54
Practical Money Skills	https://privacy.commonsense.org/evaluation/Practical-Money-Skills	Warning	49	39
Privo	https://privacy.commonsense.org/evaluation/privo	Warning	54	44
Prodigy	https://privacy.commonsense.org/evaluation/prodigy	Warning	87	58
Quizlet	https://privacy.commonsense.org/evaluation/quizlet	Warning	66	59
Raise.me	https://privacy.commonsense.org/evaluation/raise.me	Warning	59	45
ReadTheory	https://privacy.commonsense.org/evaluation/readtheory	Warning	68	50
ReadWorks	https://privacy.commonsense.org/evaluation/ReadWorks	Warning	50	36
Reddit	https://privacy.commonsense.org/evaluation/Reddit	Warning	51	51
Remind	https://privacy.commonsense.org/evaluation/remind	Pass	94	76
Ring	https://privacy.commonsense.org/evaluation/Ring	Warning	44	40
Roblox	https://privacy.commonsense.org/evaluation/Roblox	Warning	71	63
Roku	https://privacy.commonsense.org/evaluation/Roku	Warning	51	41
Samsung Galaxy Watch	https://privacy.commonsense.org/evaluation/Samsung-Galaxy-Watch	Warning	50	48
SAT Vocab by MindSnacks	https://privacy.commonsense.org/evaluation/sat-vocab-by-mindsnacks	Warning	46	40
Scholastic	https://privacy.commonsense.org/evaluation/Scholastic	Warning	75	57
Scholastic Kids	https://privacy.commonsense.org/evaluation/Scholastic-Kids	Pass	71	49
School Friendzy	https://privacy.commonsense.org/evaluation/school-friendzy	Warning	37	30
Schoology	https://privacy.commonsense.org/evaluation/schoology	Warning	63	47
Schoolzilla	https://privacy.commonsense.org/evaluation/schoolzilla	Warning	57	45
Scribd	https://privacy.commonsense.org/evaluation/scribd	Warning	44	38
Securly	https://privacy.commonsense.org/evaluation/securly	Warning	68	49
Seesaw: The Learning Journal	https://privacy.commonsense.org/evaluation/seesaw:-the-learning-journal	Pass	82	65
Sesame Street	https://privacy.commonsense.org/evaluation/Sesame-Street	Pass	63	44
Signal - Private Messenger	https://privacy.commonsense.org/evaluation/Signal—Private-Messenger	Warning	38	28
Skype	https://privacy.commonsense.org/evaluation/Skype	Warning	69	60
Slack	https://privacy.commonsense.org/evaluation/slack	Warning	59	45
Snapchat	https://privacy.commonsense.org/evaluation/Snapchat	Warning	56	52
Socrative	https://privacy.commonsense.org/evaluation/socrative	Warning	79	60

Spotify Music	https://privacy.commonsense.org/evaluation/spotify-music	Warning	56	54
StackUp	https://privacy.commonsense.org/evaluation/stackup	Pass	85	49
Summit Learning	https://privacy.commonsense.org/evaluation/Summit-Learning	Pass	91	69
Survey Monkey	https://privacy.commonsense.org/evaluation/survey-monkey	Warning	62	56
Sushi Monster	https://privacy.commonsense.org/evaluation/sushi-monster	Warning	76	62
Telegram Messenger	https://privacy.commonsense.org/evaluation/Telegram-Messenger	Warning	51	43
ThingLink	https://privacy.commonsense.org/evaluation/thinglink	Warning	76	60
Thrively	https://privacy.commonsense.org/evaluation/Thrively	Warning	75	54
TikTok - Real Short Videos	https://privacy.commonsense.org/evaluation/TikTok—Real-Short-Videos	Warning	60	50
Tubi	https://privacy.commonsense.org/evaluation/Tubi-TV	Warning	54	43
Turnitin	https://privacy.commonsense.org/evaluation/turnitin	Warning	72	57
Twitch	https://privacy.commonsense.org/evaluation/Twitch	Warning	57	49
Twitter	https://privacy.commonsense.org/evaluation/Twitter	Warning	53	50
Udacity	https://privacy.commonsense.org/evaluation/Udacity	Warning	53	51
Udemy	https://privacy.commonsense.org/evaluation/udemy	Warning	62	54
Understood	https://privacy.commonsense.org/evaluation/Understood	Warning	47	44
Valve Index	https://privacy.commonsense.org/evaluation/Valve-Index	Warning	44	44
Venmo	https://privacy.commonsense.org/evaluation/Venmo	Warning	59	50
VoiceThread	https://privacy.commonsense.org/evaluation/voicethread	Pass	87	66
Waggle	https://privacy.commonsense.org/evaluation/waggle	Pass	87	63
WhatsApp Messenger	https://privacy.commonsense.org/evaluation/WhatsApp-Messenger	Warning	66	51
Wikipedia.org	https://privacy.commonsense.org/evaluation/Wikipedia.org	Pass	63	57
Wolfram Alpha	https://privacy.commonsense.org/evaluation/Wolfram-Alpha	Warning	50	37
YouTube	https://privacy.commonsense.org/evaluation/YouTube	Warning	69	64
YouTube Kids	https://privacy.commonsense.org/evaluation/YouTube-Kids	Warning	81	69
Zoom	https://privacy.commonsense.org/evaluation/Zoom	Warning	72	62
Zoom for Education	https://privacy.commonsense.org/evaluation/Zoom-for-Education	Pass	87	73

List of Products Evaluated all four years

Product	Evaluation URL	Rating	Basic Score	Full Score
Accelify	https://privacy.commonsense.org/evaluation/accelify	Warning	41	31
Achieve3000 Literacy Solutions	https://privacy.commonsense.org/evaluation/achieve3000-literacy-solutions	Pass	96	66
Actively Learn	https://privacy.commonsense.org/evaluation/actively-learn	Warning	72	50
Akindi	https://privacy.commonsense.org/evaluation/akindi	Warning	37	28
Amazon Kindle	https://privacy.commonsense.org/evaluation/Amazon-Kindle	Warning	62	54
Angry Birds	https://privacy.commonsense.org/evaluation/angry-birds	Warning	57	46
Animoto	https://privacy.commonsense.org/evaluation/animoto	Warning	71	61
Bloomz	https://privacy.commonsense.org/evaluation/bloomz	Warning	69	52
Brainquake	https://privacy.commonsense.org/evaluation/brainquake	Warning	47	43
Canvas	https://privacy.commonsense.org/evaluation/canvas	Warning	63	46
Capit	https://privacy.commonsense.org/evaluation/capit	Pass	79	66
Class Charts	https://privacy.commonsense.org/evaluation/class-charts	Warning	49	37
Class123	https://privacy.commonsense.org/evaluation/class123	Warning	35	33
ClassDojo	https://privacy.commonsense.org/evaluation/classdojo	Pass	90	74
ClassFlow	https://privacy.commonsense.org/evaluation/classflow	Pass	87	69
Classkick	https://privacy.commonsense.org/evaluation/classkick	Pass	93	69
Clever	https://privacy.commonsense.org/evaluation/Clever	Pass	91	69
Code Combat	https://privacy.commonsense.org/evaluation/code-combat	Warning	60	42
Code.org	https://privacy.commonsense.org/evaluation/code.org	Pass	96	77
CodeHS	https://privacy.commonsense.org/evaluation/codehs	Warning	63	48
Curious World - Early learning games, videos and books for kids	https://privacy.commonsense.org/evaluation/curious-world—early-learning-games,-videos-and-books-for-kids	Warning	40	38
Desmos	https://privacy.commonsense.org/evaluation/desmos	Pass	87	69
Dictionary.com	https://privacy.commonsense.org/evaluation/dictionary.com	Warning	57	54
Duolingo	https://privacy.commonsense.org/evaluation/duolingo	Warning	57	48
EasyBib	https://privacy.commonsense.org/evaluation/easybib	Warning	56	50
Edmodo	https://privacy.commonsense.org/evaluation/edmodo	Warning	69	58
EDpuzzle	https://privacy.commonsense.org/evaluation/edpuzzle	Pass	91	73
Edsby	https://privacy.commonsense.org/evaluation/edsby	Pass	87	55
Edthena	https://privacy.commonsense.org/evaluation/edthena	Pass	81	64
Edulastic	https://privacy.commonsense.org/evaluation/edulastic	Pass	94	59
edWeb	https://privacy.commonsense.org/evaluation/edweb	Warning	68	47
EvaluationKIT	https://privacy.commonsense.org/evaluation/evaluationkit	Warning	54	48

Explain Everything	https://privacy.commonsense.org/evaluation/explain-everything	Pass	88	72
Flocabulary	https://privacy.commonsense.org/evaluation/flocabulary	Pass	93	70
Formative	https://privacy.commonsense.org/evaluation/formative	Pass	93	66
Gaggle	https://privacy.commonsense.org/evaluation/gaggle	Pass	78	56
Goodreads	https://privacy.commonsense.org/evaluation/goodreads	Warning	50	34
i-Ready	https://privacy.commonsense.org/evaluation/i-ready	Pass	84	58
Instagram	https://privacy.commonsense.org/evaluation/instagram	Warning	57	49
Istation	https://privacy.commonsense.org/evaluation/istation	Warning	51	38
Kahoot!	https://privacy.commonsense.org/evaluation/kahoot	Pass	76	64
Kami	https://privacy.commonsense.org/evaluation/kami	Pass	90	65
Khan Academy	https://privacy.commonsense.org/evaluation/khan-academy	Pass	88	71
Lynda	https://privacy.commonsense.org/evaluation/lynda	Warning	53	40
Matific	https://privacy.commonsense.org/evaluation/matific	Warning	72	54
MobyMax	https://privacy.commonsense.org/evaluation/MobyMax	Warning	56	40
Nearpod	https://privacy.commonsense.org/evaluation/nearpod	Warning	88	65
Nitro Type	https://privacy.commonsense.org/evaluation/nitro-type	Warning	41	33
NoRedInk	https://privacy.commonsense.org/evaluation/noredink	Warning	93	90
Pinterest	https://privacy.commonsense.org/evaluation/Pinterest	Warning	50	49
Plickers	https://privacy.commonsense.org/evaluation/plickers	Warning	57	46
Privo	https://privacy.commonsense.org/evaluation/privo	Warning	54	44
Prodigy	https://privacy.commonsense.org/evaluation/prodigy	Warning	87	58
Quizlet	https://privacy.commonsense.org/evaluation/quizlet	Warning	66	59
Raise.me	https://privacy.commonsense.org/evaluation/raise.me	Warning	59	45
ReadTheory	https://privacy.commonsense.org/evaluation/readtheory	Warning	68	50
Remind	https://privacy.commonsense.org/evaluation/remind	Pass	94	76
Schoology	https://privacy.commonsense.org/evaluation/schoology	Warning	63	47
Schoolzilla	https://privacy.commonsense.org/evaluation/schoolzilla	Warning	57	45
Scribd	https://privacy.commonsense.org/evaluation/scribd	Warning	44	38
Securly	https://privacy.commonsense.org/evaluation/securly	Warning	68	49
Seesaw: The Learning Journal	https://privacy.commonsense.org/evaluation/seesaw:-the-learning-journal	Pass	82	65
Socrative	https://privacy.commonsense.org/evaluation/socrative	Warning	79	60
StackUp	https://privacy.commonsense.org/evaluation/stackup	Pass	85	49
Survey Monkey	https://privacy.commonsense.org/evaluation/survey-monkey	Warning	62	56
Udemy	https://privacy.commonsense.org/evaluation/udemy	Warning	62	54
Wikipedia.org	https://privacy.commonsense.org/evaluation/Wikipedia.org	Pass	63	57

Product Population Demographics

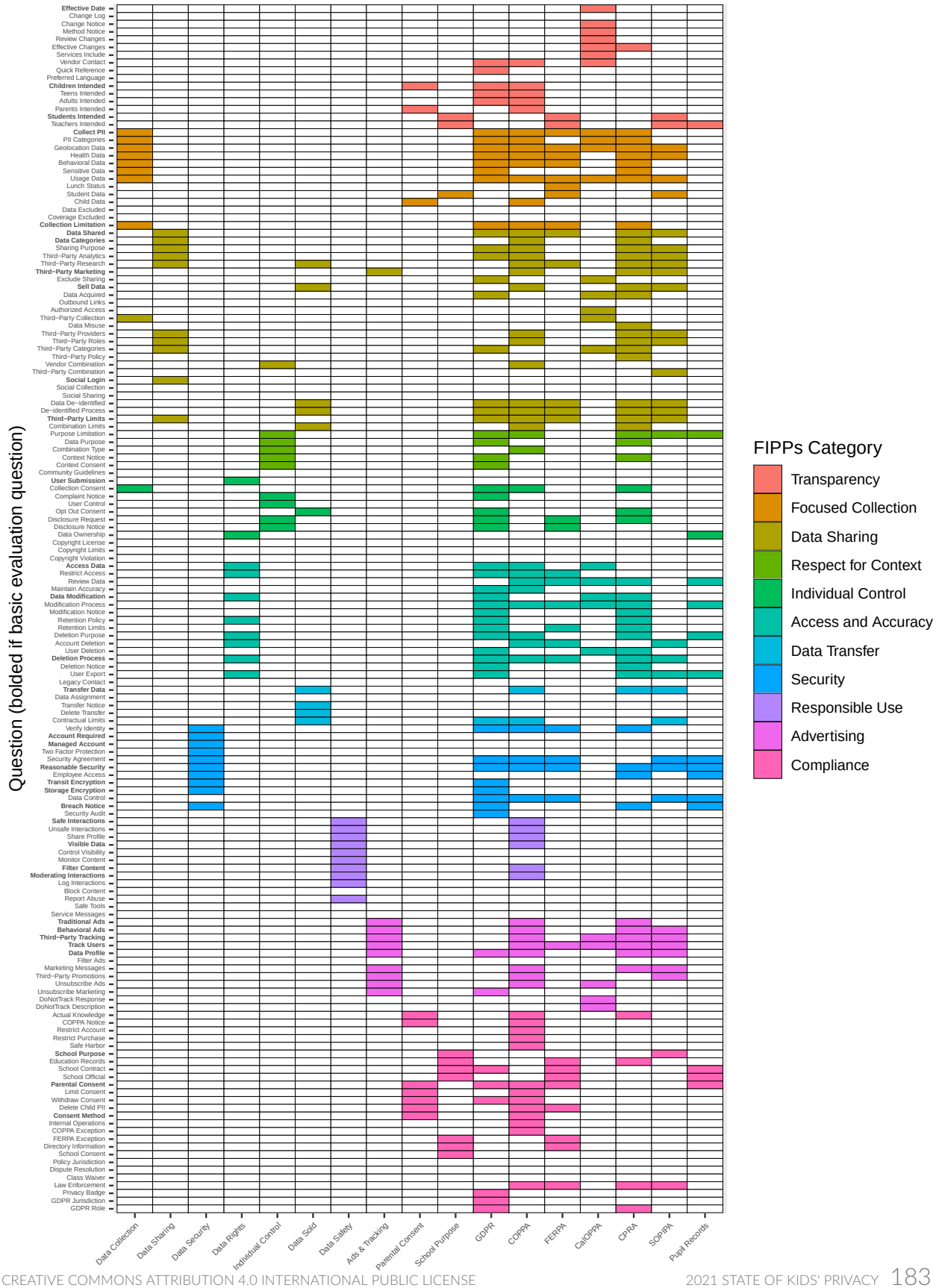
In 2020, our products evaluated changed considerably, both in terms of the number of products evaluated increasing from 150 in 2019 to 200 in 2020 and in terms of what products we evaluated. Prior to 2020, our State of Edtech Privacy reports focused primarily on educational technology products. In 2020 we expanded the products considered to include those more representative of what kids, families, and educators are using. In order to evaluate whether any changes we were seeing were heavily influenced by the 33% increase in products in a different focus than those evaluated in our historical data, we computed a chi-squared test of independence for each question response in 2020 to determine if the products we added in 2020 were notably different than those products that were evaluated in both 2019 and 2020. For each evaluation, we calculated whether or not the respective product was also evaluated in 2019 and then performed a chi-squared test to see if being evaluated in both 2019 and 2020, or only in 2020, resulted in notably different question responses in 2020. We used the calculated p-value from the chi-squared test to assist in our consideration of whether or not changes were likely to be due to our change in population or could reasonably be considered as shifts in industry practices. Low p-values (< 0.05) indicate a high likelihood that the shift in population is likely responsible for any large shifts we see in the question response data. The p-value helped inform our analysis especially with respect to whether or not any trends we may be seeing were reflective of industry changes or to changes to our process and product selection criteria. Unsurprisingly, we see questions related to schools and students with low p-values, indicating that our shift in products included is likely creating any large shifts in responses since 2019.

Question	Chi-square p-value
Effective Changes	0.0000
Students Intended	0.0000
Teachers Intended	0.0000
Student Data	0.0000
Third-Party Policy	0.0000
School Purpose	0.0000
School Consent	0.0000
Data Assignment	0.0001
School Contract	0.0001
School Official	0.0001
Sensitive Data	0.0003
Education Records	0.0003
Collection Consent	0.0004
Outbound Links	0.0014
User Control	0.0020
Filter Ads	0.0026
Delete Transfer	0.0032
FERPA Exception	0.0033
Third-Party Marketing	0.0063
User Export	0.0075
Monitor Content	0.0081
COPPA Exception	0.0085
Behavioral Data	0.0091
Health Data	0.0095
Restrict Account	0.0096
Track Users	0.0113
Third-Party Categories	0.0137
Complaint Notice	0.0141
Data Control	0.0148
Third-Party Promotions	0.0176
Unsafe Interactions	0.0187
Filter Content	0.0201
Unsubscribe Ads	0.0269
Data Profile	0.0271
Verify Identity	0.0274
Sell Data	0.0370
Quick Reference	0.0391
Service Messages	0.0401
Disclosure Request	0.0409
Third-Party Tracking	0.0428
Third-Party Research	0.0455
Transfer Notice	0.0469
Breach Notice	0.0474
Opt Out Consent	0.0475
Data Categories	0.0489
Preferred Language	0.0492
Traditional Ads	0.0506
Parents Intended	0.0514
Data De-identified	0.0545
DoNotTrack Description	0.0655

Change Log	0.0656
Directory Information	0.0767
Geolocation Data	0.0827
Legacy Contact	0.0882
Behavioral Ads	0.0918
Social Login	0.1184
User Deletion	0.1213
Modification Process	0.1302
Retention Limits	0.1328
GDPR Role	0.1330
Privacy Badge	0.1331
Block Content	0.1406
Visible Data	0.1466
Retention Policy	0.1483
Data Purpose	0.1569
Class Waiver	0.1587
Share Profile	0.1596
Limit Consent	0.1640
Internal Operations	0.1652
Review Changes	0.1852
DoNotTrack Response	0.1887
Delete Child PII	0.1900
Third-Party Combination	0.2057
Combination Limits	0.2180
Maintain Accuracy	0.2268
Exclude Sharing	0.2424
Storage Encryption	0.2664
Copyright License	0.2817
Safe Harbor	0.2913
Teens Intended	0.3029
Authorized Access	0.3093
Third-Party Providers	0.3093
De-identified Process	0.3093
Third-Party Analytics	0.3166
Lunch Status	0.3183
Data Acquired	0.3206
Control Visibility	0.3211
Usage Data	0.3216
Sharing Purpose	0.3224
Vendor Combination	0.3341
Social Sharing	0.3378
Account Required	0.3392
Copyright Violation	0.3460
Consent Method	0.3564
Collect PII	0.3659
Log Interactions	0.3730
Context Consent	0.3749
Social Collection	0.3837
Deletion Notice	0.3856
Change Notice	0.3912
Actual Knowledge	0.4033
Moderating Interactions	0.4054
Child Data	0.4149
Managed Account	0.4169
Reasonable Security	0.4373
Data Modification	0.4432
Parental Consent	0.4456
Disclosure Notice	0.4514
Report Abuse	0.4555
Third-Party Collection	0.4732
Law Enforcement	0.4841
PII Categories	0.4906
Purpose Limitation	0.4995
Data Misuse	0.5202
Transfer Data	0.5240
Transit Encryption	0.5620
Contractual Limits	0.6012
GDPR Jurisdiction	0.6313
Services Include	0.6503
Vendor Contact	0.6602
Restrict Access	0.6704
Third-Party Roles	0.6721
Community Guidelines	0.6889
Deletion Process	0.6939
Data Ownership	0.6977
Unsubscribe Marketing	0.6991
Effective Date	0.7091
Safe Tools	0.7285
Data Excluded	0.7466
COPPA Notice	0.7473
Account Deletion	0.7524
Collection Limitation	0.7665
Review Data	0.7675
Context Notice	0.7902

Policy Jurisdiction	0.8208
Method Notice	0.8214
Security Audit	0.8349
Children Intended	0.8372
Copyright Limits	0.8430
Restrict Purchase	0.8456
Coverage Excluded	0.8638
User Submission	0.8648
Modification Notice	0.8763
Marketing Messages	0.8794
Adults Intended	0.8817
Access Data	0.8998
Third-Party Limits	0.9121
Combination Type	0.9143
Security Agreement	0.9279
Employee Access	0.9289
Dispute Resolution	0.9547
Deletion Purpose	0.9633
Data Shared	1.0000
Two Factor Protection	1.0000
Safe Interactions	1.0000
Withdraw Consent	1.0000

Figure 227: Question Map: How various questions map to Statutes and Concerns. Coloring indicates which FIPPs category a question pertains to. Bolded question names indicate they are part of a basic evaluation.



OUR OFFICES

San Francisco Headquarters
699 8th Street, Suite C150
San Francisco, CA 94103

Washington, D.C. Office
2200 Pennsylvania Avenue, NW
4th Floor East
Washington, D.C. 20037

New York Office
2160 Broadway, 4th Floor
New York, NY 10024

Los Angeles Office
1100 Glendon Avenue, 17th Floor
Los Angeles, CA 90024

London Office
Exmouth House
3/11 Pine Street
Farringdon, London EC1R 0JH
United Kingdom

common sense®

www.commonsense.org