2021

# STATE OF KIDS' PRIVACY

KEY FINDINGS

common sense®

# 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.

**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

[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.

[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.