Utah EdTech App Data Collection and Sharing: 2023-25 Investigation

A project in partnership between the Utah State Board of Education and researchers at Brigham Young University and Internet Safety Labs

August 20, 2025

- **Mark Keith, Brigham Young University, Provo, UT, mark_keith@byu.edu*
- *Justin Giboney, Brigham Young University, Provo, UT, justin_giboney@byu.edu*
- *Lisa LeVasseur, Internet Safety Labs, San Diego, CA, lisa.levasseur@internetsafetylabs.org*
- *Bryce Simpson, Internet Safety Labs, San Diego, CA, bryce.simpson@internetsafetylabs.org*

* Corresponding author

Table of Contents

Executive Summary

The purpose of this project is to measure and understand the current state of student data privacy associated with the educational technology (EdTech) applications used in the state of Utah. This includes assessing 1) a list of the apps being used, 2) the compliance with data privacy agreements by app companies that have signed them, and 3) the actual data collection and observed sharing of all apps. To accomplish this, researchers from Brigham Young University and Internet Safety Labs have aggregated data from a variety of sources, including an investigation of the actual network traffic that contains student, parent, and teacher data sent from the EdTech apps used throughout the state. The results included in this report indicate that while there is some adherence to data privacy agreements in terms of which data fields are being collected by the EdTech companies, some apps are collecting data elements that are not included in privacy agreements and sharing this data with third parties, including advertisers. These results led to a significant effort to meet with EdTech vendors and reconcile the differences. Their responses ranged from very positive (in most cases) to undesirable (such as ignoring the request entirely).

Background and Motivation

The industry for instructional or educational technology (EdTech) grew exponentially to a global market size of approximately $123.4 bn USD in 2022 and is expected to reach $348.41 bn by 2030 (GrandViewResearch.com, 2023). This growth continues to occur despite significant information privacy risks. For example, Internet Safety Labs (2023) recently tested and analyzed network traffic from 1,357 popular EdTech apps and found that student, parent, and teacher data were being sent to third parties by 96 percent of the apps, and that 78 percent of the apps exhibited data sharing that was so egregious that they were designated as “Do Not Use.” This is particularly disturbing considering how vast the capabilities are today for digital profiling, where data brokers create consumer profiles that can uniquely identify individuals based on their online behaviors and data sharing (Akar & Nasir, 2015; van Dam & Van De Velden, 2015).

There is little doubt that EdTech apps[1], when used appropriately, offer considerable benefits for student learning, lesson planning and preparation, time and cost efficiency, and more (Earle, 2002; Grayson, 1972; Honey et al., 2000). The objective should not be to minimize the use of EdTech apps, but only to use them safely after weighing the benefits against the privacy risks to our students (Marshall et al., 2022). The most significant barrier to this goal is the fact that the level of technical expertise, time, and resources required to objectively assess the safety of all potential EdTech apps cannot be realistically required of educators. Furthermore, technology vendors are known to conceal their data collection and sharing practices from their consumers (Dalsen, 2009; Kemp, 2020; Schneier, 2015). Consequently, to the best of our knowledge, no other researchers have uncovered the data collection and sharing practices of EdTech vendors. Similar research has been performed in other disciplines, such as healthcare (Grundy et al., 2019) and consumer apps (Pimienta et al., 2023), and has revealed that extensive potentially illegal data collection and sharing do occur.

While the state of Utah has already taken significant steps to require privacy standards from EdTech vendors, the purpose of this project is to collect and aggregate data that will help the Utah State Board of Education (USBE) understand whether EdTech vendors are currently meeting their student privacy obligations. Each app is approved under one of several criteria that may include data privacy agreements (DPAs) that contractually allow app companies to collect specific student data elements. A few apps may collect data elements outside of these agreements and even share them with third parties against the DPAs. This includes advertising-related (AdTech) and marketing-related (MarTech) companies. Other apps specify in their agreements that they will collect data but are vague in their interpretations, which makes it impossible for teachers and administrators to make informed adoption decisions. Finally, many app companies do behave ethically and currently abide by their agreements.

Beginning in the summer of 2023, the researchers first collected a list (as comprehensive as possible) of the EdTech apps being used throughout Utah and of those DPAs that vendors had signed. We identified over 3,000 unique apps being used at the time of that collection. We then selected 100 of these apps based on a variety of criteria (e.g., most frequently used, Utah-based apps vs. external, apps with DPAs vs. those without, apps requiring authentication vs. those that do not). These apps were investigated

[1] We use the term “apps” to refer to both mobile- and computer-based apps as well as websites because each type of “app” can collect and share data in the same way including allowing users to create accounts that specify their age.

using an Internet/network traffic communications “sniffing” technique to identify *what* data was sent from EdTech apps and to *where* it was sent.

Network traffic testing has been commonly used in prior research to verify the data collection and sharing practices of app vendors including those who provide apps for children (e.g. Grundy et al., 2019; Joshi et al, 2015; Jibb et al., 2022). Network traffic testing is distinct from code auditing, which we did not perform on any app. Network traffic testing allows us to accomplish only the necessary objective of determining which data elements are collected and where the data is sent without violating code copyrights or requiring any form of white- or black-hat “hacking” (Joshi et al., 2015). This testing methodology was only performed on our own networks and machines to be compliant with Electronic Communications Privacy Act (ECPA). The process included observing the plain text data these apps sent from our device and the Internet Protocol (IP) address of the location it was sent to. These IP addresses were matched with domain names found in public domain servers to determine which companies were receiving this data. No “decrypting” was performed or required. Where necessary, we used a “dummy” student account with permission so that no real student data would be exposed.

We broadly categorize the network traffic testing results into three groups: 1) apps that are compliant with their data privacy agreements or policies; 2) apps that are violating existing agreements (minimally in certain cases and significantly in others); and 3) apps that may or may not be noncompliant, which we recommend be further examined by those with legal expertise, such as state attorneys.

By testing 100 apps, we demonstrated that network traffic testing, or investigations, can reveal EdTech app (non)compliance that cannot be objectively measured in any other manner. We recommend that the USBE carefully consider how these results can be used to aid teachers and administrators in their future EdTech adoptions. Through cooperative efforts with the USBE Data Privacy team, a process has been developed to work with EdTech vendors to reconcile the differences found between signed DPAs, agreements, and privacy policies and the actual results of network traffic testing. Because this process has been extremely valuable, we recommend the State of Utah provide continuing support to this group as future testing and alignment will almost certainly be needed. Lastly, we commend the USBE for leading this initiative that values the interests of the students—a potentially vulnerable population in terms of data privacy (McDonald & Forte, 2022). We recommend continuing the initiative by continuing to collect objective reports on EdTech provider practices so that teachers and administrators can make fully informed adoption decisions.

In the remainder of this report, we first review the existing privacy efforts and governance structures within the state. Next, we review various privacy regulations that are relevant to our findings. Then, we review the three phases of this project, including their results and findings. Finally, we conclude with a high-level summary of the project. We note that the overall purpose of this project was to generate an objective snapshot of the state of EdTech privacy practices compared to the legal agreements in place. Specific actions and “next steps” should be determined by those with legal expertise and positions of authority in this field.

Review of Existing Privacy Efforts

The State of Utah has made significant progress regarding student data privacy in recent years, which should be noted.

The Birth of Utah's Student Data Protection Act

In 2016, the Utah legislature passed H.B. 358 Student Privacy Amendments, which established the Student Data Protection Act (SDPA) (HB358, 2016). This new law required the USBE and local education agencies (LEAs, i.e., districts and charter schools) to adopt data governance and privacy practices. Additionally, the law put in place requirements and restrictions for any third-party provider that receives students' personally identifiable information from the USBE or an LEA. The law also provided funding to employ a chief privacy officer for USBE.

Expanded Privacy Program at USBE

The following year, the USBE received additional funding that allowed the agency to hire additional privacy team members and fund the creation of the state's original metadata dictionary (MDD). The additional team members enabled the data privacy team to provide training to LEAs, including responding to gaps in the knowledge of LEAs by producing individualized training and engaging videos. This helped the LEAs develop an understanding of privacy laws and best practices.

Metadata Dictionary (MDD) Requirement and Data Privacy Agreements (DPAs)

One of the established requirements in Utah's Student Data Protection Act (SDPA) is for the USBE and each LEA to maintain a metadata dictionary (MDD). This MDD is a listing of third parties that receive student personally identifiable information (PII) from the agency, along with information regarding the purpose for sharing the data. For many LEAs, most of the entities that receive student PII are EdTech companies. Thus, an LEA's MDD often acts as a list of approved EdTech applications in use in LEAs.

Additionally, the SDPA requires LEAs to ensure that their contracts with third-party vendors include certain provisions. Obtaining a DPA is the most common method used by LEAs to meet this obligation. Most LEAs use their MDD to log and document the DPAs they have in place with EdTech providers.

History of Growth

Each fall, the student data privacy team at the USBE conducts the Annual Privacy Compliance Review. In this annual monitoring, each LEA in the state is required to submit evidence of its compliance with privacy laws. Every year, the USBE slightly expands the requirements for districts and charter schools to encourage growth. Findings from the Annual Privacy Compliance Review suggest ongoing improvement in the LEAs' compliance, particularly regarding the MDD requirement.

The two charts in Figures 1 and 2 below depict the rise in compliance over the last three years of the Annual Privacy Compliance Reviews. Each year, after receiving their results, the LEAs participate in trainings and individualized coaching to help them attain compliance in subsequent years.

Plans for future Annual Privacy Compliance Reviews include a more rigorous self-assessment and ongoing attention to compliance with MDD requirements.

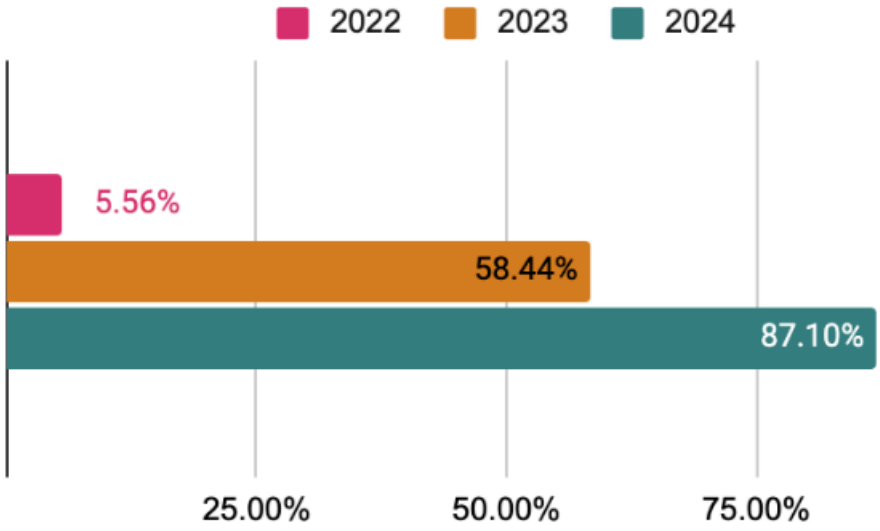

Figure 1. MDD Compliance in all Utah LEAs Over Time

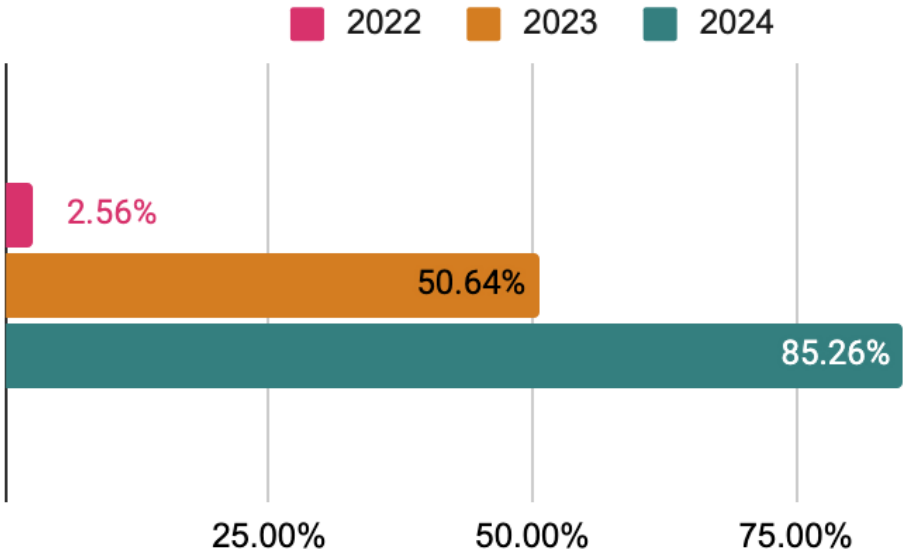

Figure 2. Overall Compliance in Utah LEAs Over Time

Utah's Privacy Future

While Utah has always valued data privacy, the USBE student data privacy team has observed that LEA privacy practices are constantly improving. The team has identified the following trends as they work with LEAs across the state:

- **Privacy Review.** An increasing number of LEAs are building a formal privacy review into their app-vetting processes.
- **Responding to Parent Feedback.** LEAs are becoming increasingly responsive to parents' privacy concerns. They are improving their transparency and communication regarding data collection and utilization.

- **Insistence on DPAs.** LEAs are showing a growing determination to ensure that DPAs are in place with all vendors they utilize.
- **Improving Practices.** LEAs are moving from meeting the minimum requirements of privacy law to more broadly improving privacy practices.

Regulations, Policies, Contracts, and Agreements

Although we have already mentioned Utah's SDPA regulations above, there are several other relevant regulations, which we will review here, that should be understood to help interpret the results of this investigation. It must be noted that this review does not constitute legal advice or guidance, as the authors are not lawyers; this review is simply a reference point for interpreting the results reported subsequently.

The Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA, 1998) applies specifically to children aged under 13 years and their data privacy while using online services. It requires that EdTech providers obtain verifiable parental consent before collecting personal information from children. Please note that the Federal Trade Commission (FTC) has specified that schools can also grant consent on behalf of parents (FTC, 2013, Section N). COPPA outlines what must be included in privacy policies, including how operators will use the collected data. It also provides parents with the ability to review what information has been collected about their children and what they want deleted. COPPA is enforced by the Federal Trade Commission (FTC).

COPPA is most relevant to this report because it strictly prohibits the following activities without parental consent:

1) *Targeted advertising*: The use of personal information from children to target specific ads based on that information.
2) *Behavioral advertising*: The use of persistent identifiers (e.g., cookies, IP addresses, and other unique user identifiers [UUID]) that allow children to be tracked over time and across different websites or online services for the purpose of profiling and targeting them with ads.
3) *Disclosure to third parties*: The personal information of children aged under 13 years cannot be shared with third parties.
4) *Geolocation information*: Collecting and using geolocation information for targeted advertising.

Advertising, third-party disclosure, and geolocation information are each relevant to the present investigation, as will be demonstrated subsequently in the report.

The Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA, 1974) specifically protects the privacy of student educational records. It outlines certain parental rights regarding their children's education records, which then transfers back to the student when they attain the age of 18 years or attend a school beyond the

high school level. It requires written consent from parents or eligible students to release any information from a student's education record, and it is enforced by the U.S. Department of Education.

There are certain cases in which FERPA allows data sharing without student or parental consent. For example, academic records can be shared with school officials with legitimate educational interests, other schools to which the student is transferring, specified officials for audit or evaluation purposes, organizations conducting approved studies, accrediting organizations, or law enforcement officials with lawfully issued subpoenas. In addition, certain information can be shared for health and safety emergencies, directory information, financial aid, and when state and local authorities within a juvenile justice system make requests to this effect (FERPA, 1974, 34 CFR § 99.31(a)). Further, LEAs may share data with vendors under relevant exceptions, but vendors are required to only use, collect, and share data for the purposes outlined in their agreement with the LEA and may not disclose information beyond the scope of their agreement. In other words, EdTech vendors should not unilaterally collect data that is not explicitly allowed by school officials and neither should they share any of that data with unauthorized third parties. As will be demonstrated later, this is occurring among many EdTech vendors.

The Utah Student Data Protection Act (SDPA)

The Utah SDPA (SDPA, Title 53E, Chapter 9, Sections 301–310) sets out specific guidelines and requirements for the protection and management of student data in Utah. The act defines several key terms, such as necessary student data, optional student data, and personally identifiable student data. *Necessary student data* refers to data required by state or federal law for educational activities, including personal details such as name, date of birth, contact information, assessment results, and more. *Optional student data* refers to data that are not essential for educational activities but may include information related to individualized education programs (IEPs), biometric information, etc. *PII* refers to data that can identify a student, including names, addresses, social security numbers, and other sensitive information. We caution that recent research has demonstrated that when grouped in sufficient quantities, all data may be personally identifiable (Morehouse et al., 2024; Sweeney, 2000; Yacobson et al., 2021).

According to the SDPA, the USBE is tasked with establishing a data governance plan to oversee student data protection statewide (Section 53E-9-302, 2a). This plan—including the implementation of a chief privacy officer and staff, the use of MDDs and DPAs, and the documented growth of compliance over time—was reviewed above. From our interactions with this group and direct observance of the trainings, documentation, and recordings provided for review, our opinion is that the SDPA has been well executed in practice. In fact, this project may be considered a creative and intentional step forward by the USBE in fulfilling SDPA regulations.

It is worth explaining a few of the requirements in greater detail. First, as mentioned above, Section 53E-9-302 (2b) mandates that in addition to the statewide data governance plan, there should be a state-level MDD, which is a listing of third parties that receive student PII from LEAs and information regarding the purposes for sharing the data. In addition, each LEA must maintain their own MDD. To fulfill this requirement, the USBE allows LEAs to implement their individual MDDs in a variety of formats, which most often include registration of contracts and EdTech vendors used in either (a) the Student Data Privacy Consortium (SDPC) website, or (b) the LearnPlatform.org website, both will be discussed in depth later. The third most common option for LEAs to implement their MDD is in a Google Sheets-based template that is generated by the USBE student data privacy team.

Section 53E-9-302 (4) establishes the office of the state student data officer to manage the records created in fulfillment of the SDPA. It requires that each LEA create and maintain its own data governance plan and MDD. Section 53E-9-304 outlines that students and parents own the student data and that parents must be notified in case of significant breaches.

Section 53E-9-305 is one of the most relevant portions of our report. It states that LEAs may collect the necessary student data, and that LEAs may collect optional student data. LEAs specify which data are allowed to be collected when they sign DPA contracts with the vendor.

Sections 53E-9-306–53E-9-308 pertain to the USBE and the state data privacy manager and are not particularly relevant to this report. Section 53E-9-309 pertains to third-party contractors and is of great significance to our findings. It states that (1) EdTech vendors can only use student data "strictly for the purpose of providing the contracted product or service within the negotiated contract terms." This section also states that (2b) vendors must specify, in a contract, which additional contractors or "fourth parties" they are sharing student data with.

Section 53E-9-309 indicates that EdTech vendors may use student data for (4a) adaptive learning, (4b) marketing other EdTech products (if they did not use data from their app to customize those advertisements), (4c) using a recommendation engine to advertise learning products to students IF the recommendations are not motivated by payments (e.g., "sponsored" advertisements), (4e) improving the functionality of the app, or (4f) identifying scholarships or nonprofit higher education opportunities for the student. In addition, the vendor must (5) return or delete all student data upon the LEA's request unless the student or parent consents to allowing them to keep it. Importantly, EdTech vendors may NOT (6a) collect, use, or share student data if it is not specifically allowed in the contract.

Finally, Section 53E-9-310 indicates that individuals who knowingly or recklessly misuse student data may face penalties, including civil fines of up to $25,000 and potential criminal charges.

App-Level Agreements, Policies, Assurances, and Contracts

As specified by the SDPA, each EdTech vendor in use within the state must sign a contract with an LEA or state entity. These contracts must comply with the SDPA, which also complies with the relevant federal regulations reviewed above. Figure 3 visualizes the dynamics between each level. State regulations must fall within, or not violate, federal regulations, and app-level agreements must adhere to state- and federal-level regulations. There are a variety of privacy assurances and agreements, in addition to contracts, that are worth reviewing.

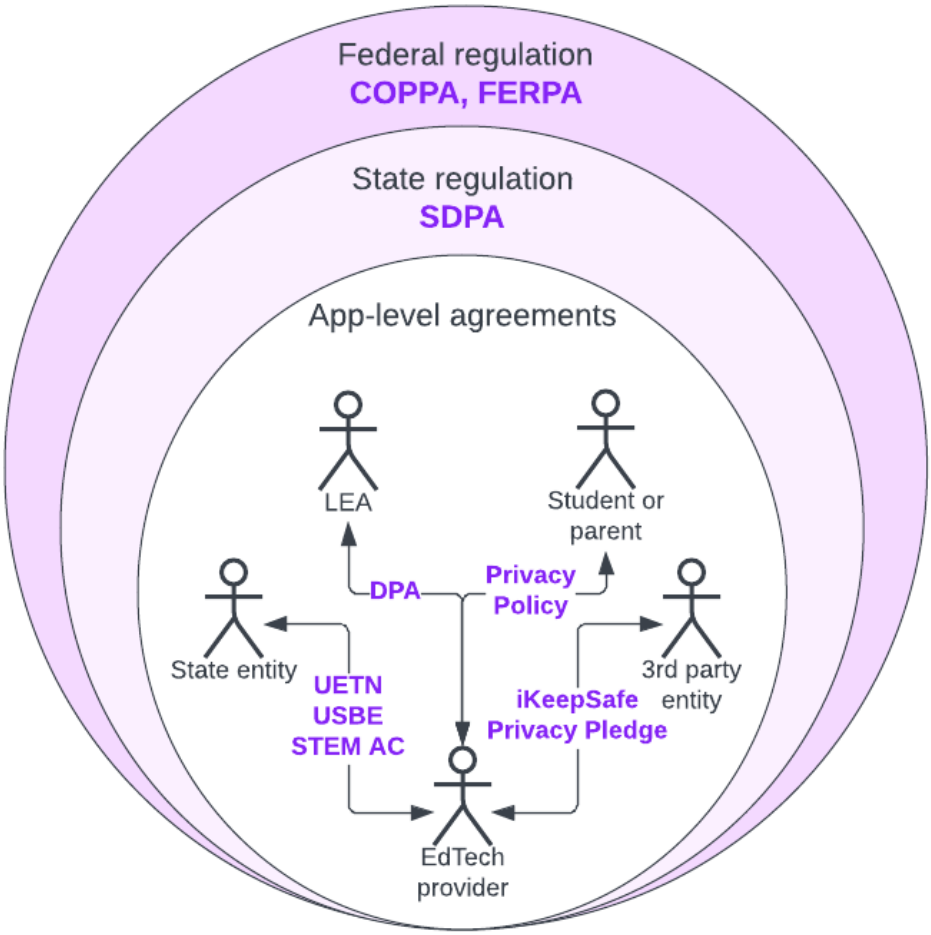

Figure 3. Conceptualization of the Dynamics Among Regulations and Agreements

The Utah Education and Telehealth Network (UETN); Utah State Board of Education (USBE); Science, Technology, Engineering, and Math (STEM) action center (AC) contracts; and DPAs

Contracts are commonly used throughout the state of Utah and are entered into by an individual EdTech provider with any one of several relevant entities. The Utah Education and Telehealth Network (UETN) is a significant organization that provides comprehensive network and technology services for education and healthcare fields across the state of Utah. As indicated by the name, UETN combines the efforts of two primary networks: the Utah Education Network (UEN) and Utah Telehealth Network (UTN). UETN signs contracts with certain providers that are used in education and qualify as “EdTech” because they transmit student data. These contracts must adhere to state and federal regulations. Once they are signed by UETN, Utah schools can use these apps. A few examples of this include Canvas, Nearpod, Adobe Creative Cloud, Utah’s Online Library, and others that may be useful across the education domain. These contracts specify that user data cannot be sold or shared with anyone other than “data subprocessors.”

The Utah State Board of Education (USBE) has also signed contracts with certain EdTech providers that are used across all (or the vast majority of) schools in the state. The format of these contracts is very similar to that of UETN contracts; a few examples include Utah Compose, Utah Aspire Plus, RISE, Dynamic Learning Maps/Kite Suite, i-Ready, and Imagine Learning.

The science, technology, engineering, and math (STEM) Action Center (STEM AC) is an initiative aimed at promoting STEM education throughout the state and is similar to UETN and USBE contracts with EdTech providers for their specific domain; a few examples of this include IXL, ALEKS, and ST Math.

Importantly, any app that has agreements with these entities can be used by any other LEA in the state. This allowance also applies to contracts signed by specific LEAs and EdTech providers. These are referred to as DPAs, which fulfill the State requirement for the SDPA (Title 53E, Chapter 9, Sections 309). The current standard DPA contract can be found here: https://sdpc.a4l.org/agreements/UT_NDPA_V1.pdf. This is one form of DPA that is provided by the SDPC.

DPAs are signed when an LEA wants to use a new EdTech that does not already have a contract signed by UETN, USBE, or STEM AC. The SDPC refers to them as “agreements” as they are supplements to existing contracts as opposed to contracts themselves.

Once one LEA signs a DPA with an EdTech provider, any other LEA can subscribe to that contract by signing an “Exhibit E," which is an optional exhibit authorized by the vendor and DPA originator.

DPAs are unique from the other contracts in terms of one key attribute. The “Exhibit B” section of DPAs specifies a list of potential student data elements (e.g., name, address, email) that may be collected and processed by the EdTech provider. Essentially, this forces the provider to disclose exactly what will be collected. While it is not necessarily required that this level of detail be spelled out in contracts (since providers must honor these requests regardless), it does make it significantly easier to investigate the data privacy practices of the provider, as will be demonstrated later in this report.

Another detail relevant to almost every contract is that data sharing is not allowed with any third party other than “subprocessors.” The language regarding subprocessors in the standard DPA contract is as follows (similar language is used in the other types of contracts—UETN, USBE, and STEM AC):

> *4. Subprocessors. Contractor shall enter into written agreements with all subprocessors performing functions pursuant to the Service Agreement, whereby the subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA. Contractor shall provide the LEA with a description of the subprocessors or types of subprocessors who have access to the LEA’s student data and shall update the list as new subprocessors are added.*

In this language, the “Contractor” refers to the EdTech app vendors. EdTech vendors have “provide[d] the LEA with a description of the subprocessors or types of subprocessors that have access to the LEA’s student data” by giving them annual copies of their privacy policies. This would only meet that obligation if their privacy policies include the list of the specific subprocessors mentioned above. It should be noted that certain vendors’ privacy policies include variations that are occasionally rather specific and vague at other times. Whether such lists meet the obligation described above should be determined by those with legal expertise in the state.

Third-Party Verifications or Agreements: Privacy Pledge and iKeepSafe

In addition to specific app-level contracts, there are two third parties that provide a level of validation or verification of EdTech providers that can be used to approve and adopt EdTech apps in the state of Utah.

First, the Student Privacy Pledge (StudentPrivacyPledge.org, 2020a) was introduced by the Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA) as a formalized commitment by EdTech providers to follow existing federal regulations regarding the collection and handling of student data. EdTech providers can "sign on" the pledge by completing an application that requires providers to report the portions of their privacy policy that apply to each portion of the pledge found here: https://studentprivacypledge.org/privacy-pledge-2-0/. According to their website (https://studentprivacypledge.org/), "the Pledge is not intended as a comprehensive privacy policy nor to be inclusive of all requirements to achieve compliance with all applicable federal or state laws."

The Student Privacy Pledge appears to be little more than a third-party verification of a privacy policy that may or may not meet federal and state requirements. There is no verification by the originators of the Student Privacy Pledge of the actual practices of those who sign the pledge. As revealed later in the results, most of the apps in use in the state of Utah whose vendors have signed the Student Privacy Pledge have also signed DPAs or other contracts. Based on the data available to us, there are a few apps in use that appear to be approved under the Student Privacy Pledge alone, including EVERFI K-12, Bloomz, Mathigon, and others.

The Student Privacy Pledge is enforceable by the FTC: "By taking the Pledge, a company is making a public statement of their practices with respect to student data. Accountability comes from the Federal Trade Commission (FTC), which has the authority to bring civil enforcement actions against companies that do not adhere to their public statements of practices. If a company acts in contradiction to their own public statements, they risk an enforcement action for 'unfair or deceptive trade practices'" (StudentPrivacyPledge.org, 2020b). This is known as "FTC Section 5 authority" (FTC, 2021).

iKeepSafe.org provides a somewhat more robust third-party verification of EdTech provider student data privacy practices. iKeepSafe performs several regulatory compliance certifications, including COPPA Safe Harbor certification, a program that is covered by the COPPA and allows organizations to create self-regulatory guidelines, which, if approved by the FTC, can offer compliance benefits to those organizations. It aims to ensure that practices around the collection, use, maintenance, and disclosure of personal information from children comply with COPPA's requirements. As a Safe Harbor certification program, iKeepSafe is obligated to perform certification per the law and is monitored and subject to enforcement by the FTC.

Like the Student Privacy Pledge, providers can apply to iKeepSafe.org. It is distinct in that it includes a "certification" process as opposed to a "pledge" or "promise" alone. While iKeepSafe.org does not provide significant details regarding its certification approval process, it does claim to use "a series of proxy and web traffic analysis tools to complete the technical assessment, depending on the environment, to reveal the third parties receiving data from the product" (iKeepSafe.org, 2024). After the web traffic analysis, the process states that "our privacy assessors will work with you to resolve any emergent privacy or security gaps to bring your product into compliance."

Although we cannot verify any of iKeepSafe's claims nor how they complete their technical assessment, this process is certainly more objective than that of the Student Privacy Pledge. Importantly, EdTech

providers pay a fee to support iKeepSafe.org, which motivates both entities to come to an agreement on the certification. Yet, we have no reason to suspect that iKeepSafe.org is anything but accurate and honest in its certification process. Again, like the Student Privacy Pledge criteria, most EdTech providers in use throughout the state of Utah that have been certified by iKeepSafe.org have also signed contracts with a certain entity in the state. Exceptions include apps such as Along, ClassFlow, Attainment Company, Kuta, and Mote.

EdTech App Provider Privacy Policies

Finally, there are a few EdTech apps in use in the state for which we were unable to find a signed contract. In such cases, while federal and state regulations apply to these apps, they can still be evaluated against the privacy policy that they offer to the consumer. Privacy policies have traditionally been more difficult to enforce as legally binding unless they meet certain conditions: their policies must be clearly and conspicuously presented; they must obtain user consent—for example, they must require users to click on “I agree”; they must also be consistent and transparent in describing the company’s data practices. With the emergence of new legislation, companies may be held legally accountable to uphold their privacy policies.

Summary

EdTech contracts, regulations, agreements, and policies are enforceable by a certain entity, such as the Department of Education, the FCC, the FTC, or the State Attorney General’s office. As stated above, the authors of this report are not legal professionals, and we stop short of theorizing on the legality of the EdTech vendors’ behavior, which is revealed later. Rather, we suggest that appropriate state entities review the results of this report and determine what actions, if any, are warranted.

Methodology

As stated above, the purpose of this project was to create a snapshot of the current state of EdTech data privacy practices juxtaposed against the data privacy agreements and legislation relevant to those data practices. To accomplish this, we divided the project into three distinct phases that guide the remainder of this report.

First, beginning in the summer of 2023, we began by discovering each of the EdTech apps used across all LEAs in the state. Second, we collected, reviewed, and codified each of the data privacy agreements that were publicly available for each EdTech app. Third, we tested the Internet communications traffic to objectively validate exactly what student-, parent-, and teacher-based data elements were being collected by the apps tested for this project. This investigation also identified which third parties the EdTech providers were sharing these data elements with.

Phase 1: Which EdTech Apps are being Used in Utah?

Data Sources

For this investigation, we examined a variety of data sources that capture different measures. Ultimately, only a few of the primary data sources were retained, but we briefly mention everything that was initially

captured. First, we collected information regarding which EdTech apps were being used throughout the state at each LEA. We collected this from several unique sources, including the three most common types of MDD tools: 1) the Student Data Privacy Consortium (SDPC) Resource Registry (https://sdpc.a4l.org/), 2) LearnPlatform.org, 3) Google Sheets completed by LEAs functioning as MDDs, and 4) district and school websites.

The SDPC registry is a nationally recognized resource designed to help educational institutions manage and communicate the privacy and security of the EdTech apps they use. LEAs may record their EdTech adoptions on SDPC.a4l.org, identify new apps, and find the data privacy agreements that are already in use in the state. The SDPC also provides a set of standard DPA contracts that are used by the state (https://sdpc.a4l.org/agreements/UT_NDPA_V1.pdf).

Further, LearnPlatform.org extends the SDPC registry by including additional evaluations on these apps that may help decision-makers. MDDs are a standard requirement per the SDPA (53E-9-303). MDDs may include a list of individual data elements (e.g., student name, address, grades, performance) that are collected by each app. It should be noted that these dictionaries reflect what is "believed" to be used by LEAs that report. Consequently, the likelihood of natural human error dictates that these MDDs may not perfectly reflect what is happening throughout the state. In addition, it is worth noting that Figure 1 indicates that significant progress is being made in MDD usage and reporting. Finally, the district and school websites often mention specific EdTech apps that were being used in the district or charter school. While we examined all 162 district and charter school websites, we did not delve into the individual school-level websites within each district.

LEAs report all EdTech apps being used—whether through the SDPC, LearnPlatform, Google Sheets template, or a bespoke solution. Each option carries the potential for reporting errors.

Results

Overall, this data collection resulted in the identification of 5,037 distinct EdTech titles. After examining each title and combining likely duplicates (i.e., misspellings and separate versions of the same title), we reduced the likely total down to approximately 3,000 apps, depending on how versions are combined. There are probably many apps being used across the state that have not been reported in any of the sources mentioned above. There are also probably many apps in our final list of 3,000 that have been discontinued. More research would be needed to obtain an exact count, and this number likely changes regularly as new adoptions are made and existing adoptions are discontinued.

Table 1 summarizes the number of apps reported or discovered to be used at each LEA in the state. This figure illustrates the potential for discrepancies, given that certain districts—like Provo—have reported as many as 2,386 EdTech apps, while others have reported zero (e.g., Winter Sports School in Park City, Utah International Charter School, Tintic, Summit Academy High School, Roots Charter High School, Pinnacle Canyon Academy, Mountain West Montessori Academy, Monticello Academy, Dual Immersion Academy, Capstone Classical Academy, C. S. Lewis Academy, Ashcreek Academy). It is important to note that Table 1 is only a snapshot of the state of LEA reporting as of the summer of 2023. Many of those who were underreporting at the time have since fully reported and others are in the process of reporting. The purpose of Table 1 is simply to accurately reflect what we were able to capture at the time of the data collection. Our impression is that LEAs, for the most part, are doing a commendable job of collecting and reporting their EdTech usage data, as this information takes time and effort to compile.

Table 1. Count of Apps Reported or Discovered by LEA

LEA	Apps	LEA	Apps
Provo (School District)	2,386	Ignite Entrepreneurship Academy	47
Jordan	954	Utah State Board of Education	47
Washington	785	Emery	46
Granite	694	Entheos Academy	46
Weber	580	Mountain View Montessori	46
Canyons	529	Mountainville Academy	46
Freedom Preparatory Academy	474	Edith Bowen Laboratory School	45
Davis	391	Odyssey Charter School	45
Park City	340	North Summit	44
Salt Lake City	300	Garfield	43
Open Classroom	297	Lincoln Academy	43
Salt Lake Center for Science Education	297	North Davis Preparatory Academy	43
Iron	288	Vista at Entrada, School of Performing Arts & Technology	43
Ogden Preparatory Academy	276	Walden School of Liberal Arts	43
Box Elder	257	Utah Virtual Academy	42
Salt Lake School for the Performing Arts	250	Bear River Charter School	41
Wasatch	221	Merit College Preparatory Academy	41
Ascent Academies of Utah	210	Wasatch Waldorf Charter School	41
Cache	204	Academy for Math, Engineering & Science	40
Millard	203	Lumen Scholar Institute	40
Grand	189	Syracuse Arts Academy	39
InTech Collegiate High School	149	Bonneville Academy	37
Murray	140	Fast Forward Charter High School	37
South Sanpete	138	Northern Utah Academy for Math, Engineering & Science	35
North Sanpete	134	Soldier Hollow Charter School	35
Channing Hall	133	Providence Hall	34
Alpine	130	Pacific Heritage Academy	33
Nebo	130	Utah Schools for Deaf & Blind	33
Hawthorn Academy	128	Jefferson Academy	32
City Academy	125	Terra Academy	31
Maria Montessori Academy	122	Valley Academy	31
Sevier	110	HighMark Charter School	30
Uintah	109	The Ranches Academy	30
Mountain Heights Academy	105	Treeside Charter School	30
Quest Academy	101	Karl G. Maeser Preparatory Academy	29
Renaissance Academy	98	Esperanza Elementary	26
Leadership Academy of Utah	95	Leadership Learning Academy	26
South Summit	94	Wayne	26
American Leadership Academy	93	Advantage Arts Academy	25
Legacy Preparatory Academy	93	Athenian eAcademy	25
North Star Academy	93	Bridge Charter	25
Success Academy	92	Excelsior Academy	25
The Center for Creativity, Innovation, and Discovery	92	Wasatch Peak Academy	25
Juab	88	Real Salt Lake Academy High School	24
Lakeview Academy	87	Utah Military Academy	24
John Hancock Charter School	82	Wallace Stegner Academy	24
Early Light Academy at Daybreak	81	Athlos Academy of Utah	23
DaVinci Academy of Science & The Arts	78	Rich	22
Tooele	77	Summit Academy	22
Kane	76	Moab Charter School	21
Canyon Grove Academy	75	East Hollywood High	19
Franklin Discovery Academy	73	Endeavor Hall	18

Itineris Early College High School	72	Uintah River High School	18
Venture Academy	72	Utah Career Path High School	18
Logan	71	Career Academy of Utah	17
Good Foundations Academy	68	Guadalupe School	16
Voyage Academy	68	Timpanogos Academy	15
Noah Webster Academy	64	Utah Arts Academy	14
Promontory School of Expeditionary Learning	64	Weber State University Charter Academy	14
Morgan	63	Navigator Pointe Academy	13
Vanguard Academy	63	St. George Academy	13
Rockwell Charter High School	62	GreenWood Charter School	12
Thomas Edison Charter School	62	Paradigm High School	12
San Juan	61	Mana Academy Charter School	10
Beaver	59	Utah Education Network	10
Canyon Rim Academy	58	Reagan Academy	9
Utah County Academy of Sciences	58	Piute	4
Ogden	57	Salt Lake Arts Academy	3
Utah Connections Academy	57	Ashcreek Academy	0
Spectrum Academy	56	C.S. Lewis Academy	0
Mountain Sunrise Academy	53	Capstone Classical Academy	0
Carbon	51	Dual Immersion Academy	0
George Washington Academy	51	Monticello Academy	0
Scholar Academy	51	Mountain West Montessori Academy	0
Duchesne	49	Pinnacle Canyon Academy	0
American Preparatory Academy	48	Roots Charter High School	0
Beehive Science & Technology Academy	48	Summit Academy High School	0
Gateway Preparatory Academy	48	Tintic	0
Weilenmann School of Discovery	48	Utah International Charter School	0
American Academy of Innovation	47	Winter Sports School In Park City	0
Daggett	47		

Table 2 presents an ordered list of the 100 most frequently used EdTech apps found in this data collection. While these are the 100 most commonly used apps in the state, they do not represent the exact list of apps tested for network traffic results. The section Phase 3: Network Traffic Results explains how the final list of 100 apps for testing was determined.

Table 2. List of Apps across Utah LEAs

1 Utah eTranscript and Record Exchange (UTREx)	51 Desmos
2 Utah Compose	52 Embrace
3 Aspire Student Information System (SIS)	53 Newsela
4 Canvas	54 Google Sheets
5 NearPod	55 Adobe Creative Cloud Express for Education
6 Dynamic Learning Maps/Kite Suite	56 Mystery Science
7 Google Classroom	57 Gizmos
8 Google Workspace for Education Fundamentals	58 Gimkit
9 Kahoot!	59 Edpuzzle
10 Utah Aspire Plus	60 Boom Cards
11 Utah Kindergarten Entry and Exit Profile (KEEP)	61 Lexia
12 Rise	62 Flip

13 ACCESS for ELLs	63 WIDA ACCESS
14 Clever	64 Typing Club
15 Adobe Creative Cloud	65 Starfall
16 ZOOM Cloud Meetings	66 Sora, by OverDrive Education
17 Khan Academy	67 YouTube
18 i-Ready	68 Reflex Math
19 Imagine Learning	69 Pear Deck
20 American College Test (ACT)	70 Utah Pre-kindergarten Entry and Exit Profile (PEEP)
21 IXL	71 SafeUT
22 Code.org	72 No Red Ink
23 Shmoop	73 mCLASS
24 Lexia Core 5	74 Generation Genius
25 Acadience	75 CK-12
26 Utah RISE Assessment Portal	76 ST Math
27 Prodigy	77 Remind: School Communication
28 Microsoft 365	78 Google Forms
29 Canva for Education	79 CommonLit
30 Utah's Online Library	80 CodeHS
31 Typing.com	81 Utah State Immunization Information System (USIIS)
32 ClassDojo	82 PowerSchool
33 Amplify	83 Padlet
34 ALEKS	84 MasteryConnect
35 Scrible	85 Lifetouch
36 Ellevation	86 Imagine Math
37 Google Docs	87 TinkerCAD
38 Learning A-Z	88 Quill
39 Canvas Network	89 Nitro Type
40 Quizlet	90 GoGuardian
41 MobyMax	91 DBA Secure Instant Payments
42 McGraw Hill Education	92 Seesaw
43 BrainPOP	93 Scratch
44 Blooket	94 Legends of Learning
45 Google Drive	95 Google Sites
46 AAPPL	96 ABCya
47 Read Works	97 LearnPlatform
48 Quizizz	98 Kami App
49 Google Slides	99 Waterford Early Learning
50 Epic!	100 Sphero Edu

We restate that the rank order in Table 2 may not be perfectly accurate, since the results are based on self-reports from LEAs at a specific time. Changes and variations in reporting are expected; in addition, EdTech usage changes over time.

Phase 2: Which Data Elements can be Collected?

DPA Exhibit B

After collecting this list of EdTech apps being used across the state, the second phase of the project began, which involved aggregating, reviewing, and codifying the various DPAs to which these apps contractually adhere. While we have already explained each type of app-level contract, policy, and third-party certification (see Figure 3), it would be relevant to explain DPAs in greater detail at this point.

The State of Utah, as a member of the Student Data Privacy Consortium (SDPC), maintains a database of student data privacy agreements (DPAs) that is accessible on its website (https://sdpc.a4l.org/). These agreements are categorized by LEAs. Once an LEA signs an agreement with an EdTech provider, an optional “Exhibit E” enables other LEAs to adopt the same privacy protections with the provider.

To collect this information, we scraped all Utah student data privacy agreements from the SDPC website. Subsequently, we manually extracted pertinent details from 3,162 PDF documents. Of these, 911 were original DPA contracts signed by an initial LEA and the remaining 2,251 were “Exhibit E” documents, where other LEAs signed onto the original DPA.

Next, we extracted information on the subscribing and originating LEAs, EdTech providers, app names, signing dates, and data schedules (which indicated which student data elements could be shared) from all 3,162 documents. We then linked the 2,251 “Exhibit E” pages to the 911 respective parent agreements through a combination of text-matching algorithms and manual verification. We applied standard data cleaning procedures, and we stored the refined and connected data in a database for further analyses.

As mentioned above, the “Exhibit B” portion of DPAs includes a list of potential data elements that may be collected by the EdTech provider. Figure 4 depicts an example of this portion of the DPA contract that was completed by Omega Labs Inc.

EXHIBIT " B"

SCHEDULE OF DATA

Instructions: Operator should identify if LEA data is collected to provide the described services. If LEA data is collected to provide the described services, check the boxes indicating the data type collected. If there is data collected that is not listed, use the "Other" category to list the data collected.

☐ We do not collect LEA Data to provide the described services.

☑ We do collect LEA Data to provide the described services.

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	☐
	Other application technology meta data-Please specify: platform, browser, build number	☑
Application Use Statistics	Meta data on user interaction with application- Please specify: Last login	☑
Assessment	Standardized test scores	☐
	Observation data	☐
	Other assessment data-Please specify: formative and summative as assigned by the teacher	☑
Attendance	Student school (daily) attendance data	☐
	Student class attendance data	☐
Communications	Online communications that are captured (emails, blog entries) teacher to teacher creator feedback	☑
Conduct	Conduct or behavioral data only to the extent a teacher creates and/or assigns a Boom Cards mini-app that collects such information	☑
	Date of Birth	☐

	Demographics	Place of Birth	☐
		Gender	☐
		Ethnicity or race	☐
		Language information (native, preferred or primary language spoken by student)	☐
		Other demographic information-Please specify: School location can be inferred from teacher's or student's email domain if a school account	☑
	Enrollment	Student school enrollment	☐
		Student grade level can be inferred if teacher provides the information	☑
		Homeroom	☐
		Guidance counselor	☐
		Specific curriculum programs may be able to be inferred from teacher assigned content	☑
		Year of graduation	☐
		Other enrollment information-Please specify:	☐
	Parent/Guardian Contact Information	Address	☐
		Email	☐
		Phone	☐
	Parent/Guardian ID	Parent ID number (created to link parents to students)	☐
	Parent/Guardian Name	First and/or Last	☐
	Schedule	Student scheduled courses	☐
		Teacher names yes, provided by the teachers	☑
	Special Indicator	English language learner information	☐
		Low income status	☐
		Medical alerts /health data	☐
		Student disability information	☐
		Specialized education services (IEP or 504)	☐
		Living situations (homeless/foster care)	☐
		Other indicator information-Please specify:	☐

Category of Data	Elements	Check if used by your system
Student Contact Information	Address	☐
	Email yes if the teacher uses an authentication method that supplies an email	☑
	Phone	☐
Student Identifiers	Local (School district) ID number where included in student email address (we do not extract it)	☑
	State ID number	☐
	Vendor/App assigned student ID number	☑
	Student app username	☑
	Student app passwords Encrypted.	☑
Student Name	First and/or Last yes as most teachers provide actual names; pseudonyms are allowed	☑
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level) yes if teacher assigns using student performance collection; teachers may avoid by using only Fast Pin assignments	☑
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐
Student Survey Responses	yes if a teacher assigns a Boom Cards mini-app that functions as a survey or questionnaire Student responses to surveys or questionnaires	☑
Student work	Student generated content; writing, pictures etc. yes short written answers; eventually student created decks	☑
	Other student work data -Please specify: fill in the blank; multiple choice; and other responsive choices	☑
Transcript	Student course grades	☐
	Student course data	☐
	Student course grades/performance scores	☐
	Other transcript data -Please specify:	☐
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐
	Other transportation data -Please specify:	☐
Other	Please list each additional data element used, stored or collected through the services defined in Exhibit A	☐

Figure 4. Sample Exhibit B from a DPA Contract

This is one of the more “complete” examples from the documents selected because it includes 20 unique data elements selected in Exhibit B. On average, the analyzed DPA contracts included only three data element selections in Exhibit B.

Results

Table 3 below presents a rank-ordered list of the most common data elements that were specified to be collected based on the Exhibit B documents that were available at the time of data collection. For example, the student’s *name* was the most common data element selected while *other transportation data* was the least common. This list and order will likely vary as new DPAs are signed.

Table 3: Rank Sorted List of Most Commonly Collected Data Types

1	Name	25	Observation data
2	IP addresses	26	Course grades
3	Meta data on user interaction with application	27	Specialized education services
4	App username	28	Homeroom
5	App passwords	29	Assignment scores
6	Grade level	30	Graduation completion info
7	Email	31	Other demographic information
8	Teacher counselor names	32	Phone
9	School enrollment	33	Income status
10	Generated content	34	Disability information
11	App assigned ID number	35	Specific curriculum programs
12	In-application performance	36	Attendance information
13	School local ID number	37	Address
14	Assessment results	38	Conduct behavior discipline incident information
15	Course data	39	Extracurricular activities
16	Gender	40	Other indicator information
17	Birth date	41	No data collected
18	Survey results	42	Living situations homeless foster care
19	Other	43	Medical health information
20	Online communications	44	Birthplace
21	Native english speaker	45	Bus assignment
22	Ethnicity	46	Pick up drop off location
23	State ID number SSID	47	Bus card ID number
24	English language learner information	48	Other transportation data

Table 3 only includes 48 of the 79 total possible data elements because 31 elements were never selected by any EdTech vendor. Table C1 of Appendix C provides a list of all 79 possible data elements for review.

Phase 3: Network Traffic Testing

Internet Safety Labs (ISL), https://internetsafetylabs.org/, is the organization primarily responsible for performing the data collection for Phase 3 of the project. ISL is a nonprofit organization that specializes in data privacy investigations of all types of apps but they focus primarily on the EdTech market. They have released several whitepapers related to EdTech investigation results (see https://internetsafetylabs.org/blog/) as well as online tools for decision-makers to evaluate potential products, which include those listed below:

- App Microscope: A database of various EdTech app network traffic tests.
  - https://appmicroscope.org/
- Privacy risk dictionary of companies.
  - https://internetsafetylabs.org/resources/references/company-privacy-risk-dictionary/
- Privacy risk dictionary of SDKs.
  - https://internetsafetylabs.org/resources/references/sdk-privacy-risk-dictionary/
- Privacy risk dictionary of domains.
  - https://internetsafetylabs.org/resources/references/domain-privacy-risk-dictionary/

Appendix B provides detailed information regarding their testing methodology, which reveals which data elements are collected by an app and which domain names or IP addresses these data are shared with. This reveals which companies, including AdTech[2] and aggregator[3] platforms, receive the data elements. The network traffic testing methodology used in this project has been well documented in academic research (Carlsson et al., 2022; Grundy et al., 2019; Joshi & Hadi, 2015; Pimienta et al., 2023; Taylor et al., 2017) and successfully used to investigate apps in other settings, such as healthcare (Grundy et al., 2019) and children's apps (Jibb et al., 2022; Pimienta et al., 2023).

As mentioned previously, 100 apps were selected for investigation based on a variety of factors. These factors include

- apps more commonly used throughout the state;
- apps with signed DPAs or that fall under some other type of contractual obligation (e.g., a standard privacy policy, Privacy Pledge, USBE or UETN contract, STEM AC, or iKeepSafe);
- a mix of apps that required authentication versus no authentication.

Consequently, a variety of apps were tested, and not the exact top 100 list of most frequently used ones.

In each testing, the profile that was created replicated that of a student under 13 years of age to see whether regulations such as the COPPA would be followed by the provider. The testing simulated 15–20 minutes of a student using the app. All relevant and available activities or interactions with the app were performed, and all network traffic was recorded. This generated a great amount of data that is provided in

[2] AdTech platforms are any kind of entity involved in the AdTech ecosystem https://www.adexchanger.com/wp-content/uploads/2010/09/LUMA-Display-Ad-Tech-Landscape-for-AdExchanger.jpg

[3] Aggregator platforms are defined by ISL as Adobe, Amazon, Apple, Facebook, Google, Microsoft, and Twitter. These companies all have advertising-related businesses and provide a wide array of services, with insufficient disclosure of data sharing across their portfolio businesses.

this report in two ways: 1) a single summary table of all app tests and 2) a set of detailed report tables for every app tested.

Summary of Network Traffic Testing Results

A summary of each app tested is presented in Table 3. Every app vendor was provided with a copy of the network traffic findings for their app(s) (see Appendix D) and given an opportunity to respond. This process is described in greater detail in the "vendor follow-up details and observations" section. Those who responded appropriately and addressed the findings within reason were given the option to have their names redacted from this report. Those vendor names have been replaced with unique identifiers in Table 3 and the remainder of this report. Others chose not to have their names redacted. This typically occurred when the network traffic testing revealed no violations or the vendor was proud to have the assurance of the report. Some did not respond adequately or at all; their names are left in Table 3 and the rest of the report. In other words, the vendor names left in the report are due to either very good results or negligence in responding to their provided results. These response categories are indicated in superscript notations (a, b, c, and d). This process of giving vendors an opportunity to respond to network traffic results required an additional 10 months to facilitate communication back and forth with the vendors after network traffic testing.

The columns in Table 3 are understood as follows. After the EdTech app name, there is a count of the number of LEAs that have reported to be using this app. The next column, labeled "DPA," contains two types of data. If the data are numeric, then it represents a count of the number of individual data elements (e.g. student name, email, grades) that are contractually allowed to be collected according to the signed DPA available in the SDPC registry. In cases where no DPA has been signed for an app, this column includes the name of the type of contract this app falls under. For example, PrivPledge implies that we could only evaluate the app against the Student Privacy Pledge. CustomDPA for Tinkercad implies we did find a DPA, but it was generated by the vendor as opposed to being the SDPC's standard DPA. Scratch also does not have a DPA, but it also does not fall under the Privacy Pledge. In such cases, we evaluated the vendor against their own privacy policy for children under 13 years of age. These are labeled as "PrivPolicy." For these types of apps, we summarize a few potential questions to be visited by those with legal expertise in interpreting contracts later in this section.

The next group of columns, under the top-level heading "Network traffic results," presents subtotals and a total of the number of data elements discovered during ISL's investigation. For example, the first column in this group, labeled "Allowed but not collected," contains a count of data elements that are contractually legal for the provider to collect but were not found to be collected in the investigation. The second column in this group, labeled "Allowed and collected," is a count of data elements that were found in the investigation as well as the DPA contract. The third column in this group, labeled "Collected but not allowed," is salmon-colored if the value is greater than zero. The purpose of doing this is to draw the reader's attention to those apps that have collected data elements—represented by the count in that column—that were found in the investigation but are not contractually allowed by the DPA. Table 3 is initially sorted in descending order by this column to highlight the frequency of unallowed data elements being collected. The fourth and last column in this group, "Total collected," is the sum of the previous two columns.

Next, the righthand side of Table 3 contains a summary of how many of those data elements that are being collected are also being shared and with whom they are being shared. Once again, the salmon

coloring of this portion of the table is intended to draw attention to violations of DPA *and* other types of contracts. For example, the first column under the “Data elements shared” heading, with the subheading “Total shared,” represents the number of data elements that were found being shared in network traffic with IP addresses other than that of the EdTech provider. DPAs and other contracts allow providers to share data with “subprocessors” who may provide additional services necessary for app functions. In other words, the presence of sharing alone does not necessarily constitute a contract violation. The next column, labeled “Not allowed,” is salmon-colored if the value is greater than zero, because even subcontractors should not have access to data elements that are not contractually allowed in the DPA. If no DPA exists, these columns are left empty (not zero).

The final two columns, under the heading “Number of recipients,” represent areas of concern or further evaluation. The first column, “Total,” is not salmon-colored, because those recipients may simply be data subprocessors. The final column, “Advertisers,” represents the number of recipients of data who are known to be advertising organizations and do not have a stated business purpose of “subprocessing” for EdTech providers.

Table 3. Summary of EdTech Apps Tested

	Count of LEAs using the app	Data Element Collection					Third Party Data Sharing			
		DPA	Network traffic results				Data elements shared		Number of recipients	
		Total allowed	Allowed, but not collected	Allowed, and collected	Collected, but not allowed	**Total collected**	Total shared	Not allowed	Total	AdTech companies
001[b] (Teacher account)	14	**8**	2	6	13	**19**	18	13	1	0
002[b]	11	**6**	5	1	6	**7**	1	1	3	3**
Loom[c]	20	**1**	0	1	5	**6**	0	0	0	0
Replit[d]	11	**0***	0	0	5	**5**	2	2	2	1
005[b]	15	**2**	0	2	4	**6**	3	1	34	32**
006[b]	32	**14**	9	5	4	**9**	1	0	19	1
Vocabulary.com[d]	15	**12**	7	5	4	**9**	0	0	0	0
008[b]	20	**21**	10	11	4	**15**	0	0	0	0
009[b]	11	**0**	0	0	4	**4**	0	0	0	0
010[b]	56	**12**	6	6	4	**10**	0	0	0	0
011[b]	18	**0***	0	0	3	**3**	2	2	3	0
Flip[d]	37	**7**	5	2	3	**5**	2	0	2	0
013[b] (student account)	15	**2**	0	2	3	**5**	0	0	0	0
014[b]	19	**24**	20	4	3	**7**	3	2	1	0
015[b] (student account)	12	**0**	0	0	3	**3**	0	0	0	0
015[b] (teacher account)	12	**0**	0	0	3	**3**	0	0	0	0
016[b]	67	**7**	1	6	2	**8**	3	0	6	5**
017[b]	47	**10**	4	6	2	**8**	3	1	4	2**
018[b]	16	**17**	14	3	2	**5**	2	0	3	0
019[b]	40	**17**	10	7	2	**9**	5	2	3	0
020[b]	83	**9**	3	6	2	**8**	1	0	5	0
021[b]	10	**11**	5	6	2	**8**	0	0	0	0
022[b]	24	**4**	3	1	2	**3**	0	0	0	0
023[b] (teacher account)	14	**9**	3	6	2	**8**	0	0	0	0
024[b]	15	**4**	1	3	2	**5**	0	0	0	0
Vocabulary Spelling City[d]	20	**8**	5	3	2	**5**	0	0	0	0
026[b]	6	**16**	10	6	1	**7**	1	0	54	54**
027[b] (first test)	11	**0***	0	0	1	**1**	1	1	9	8
028[b] (teacher account)	32	**2**	1	1	1	**2**	1	0	10	8
028[b] (student account)	32	**2**	1	1	1	**2**	1	0	10	8
029[b]	12	**11**	8	3	1	**4**	1	0	8	7**
030[b]	28	**0***	0	0	1	**1**	1	1	4	4**
031[b]	17	**7**	3	4	1	**5**	1	0	3	2**

032[b]	11	**11**	6	5	1	**6**	1	0	1	1
033[b]	4	**10**	7	3	1	**4**	4	1	4	1
034[b]	9	**8**	2	6	1	**7**	1	0	2	0
035[b]	38	**5**	1	4	1	**5**	1	0	1	0
023[b] (student account)	14	**9**	3	6	1	**7**	0	0	0	0
036[b]	15	**19**	16	3	1	**4**	1	0	15	0
037[b]	11	**6**	3	3	1	**4**	3	0	3	0
013[b] (teacher account)	15	**2**	1	1	1	**2**	0	0	0	0
Wakelet[d]	10	**11**	4	7	1	**8**	1	0	1	0
039[b]	11	**6**	3	3	1	**4**	0	0	0	0
Destiny Discover[d]	18	**29**	29	0	1	**1**	0	0	0	0
041[b]	54	**14**	10	4	0	**4**	1	0	33	33**
042[b]	10	**4**	2	2	0	**2**	1	0	11	9**
Study.com[d]	10	**16**	11	5	0	**5**	1	0	6	6
Conjuguemos[d]	9	**9**	4	5	0	**5**	1	0	5	4
045[b]	16	**25**	19	6	0	**6**	2	0	3	3
046[b]	11	**5**	1	4	0	**4**	1	0	3	3**
047[B]	26	**23**	20	3	0	**3**	1	0	3	3**
048[b]	10	**12**	6	6	0	**6**	1	0	2	2**
049[b]	9	**12**	10	2	0	**2**	1	0	3	2**
050[b]	29	**15**	11	4	0	**4**	1	0	3	2**
051[b]	15	**21**	14	7	0	**7**	3	0	3	2
052[b]	25	**27**	16	11	0	**11**	1	0	1	1**
053[b]	10	**5**	1	4	0	**4**	1	0	1	1**
054[b]	32	**13**	6	7	0	**7**	4	0	3	1**
055[b]	23	**7**	4	3	0	**3**	1	0	2	1
056[b]	9	**12**	6	6	0	**6**	1	0	1	1
GMetrix[d]	13	**10**	6	4	0	**4**	1	0	1	1
Read Theory[d]	19	**12**	8	4	0	**4**	1	0	1	0
027[b] (second test)	11	**0***	0	0	0	**0**	0	0	0	0
059[b]	39	**10**	9	1	0	**1**	1	0	2	0
060[b]	43	**10**	4	6	0	**6**	0	0	0	0
061[b]	26	**11**	9	2	0	**2**	0	0	0	0
062[b]	15	**14**	6	8	0	**8**	2	0	3	0
063[b]	10	**17**	11	6	0	**6**	0	0	0	0
Happy Numbers (Student)[d]	12	**9**	1	8	0	**8**	0	0	0	0
Happy Numbers (Teacher)[d]	12	**9**	4	5	0	**5**	0	0	0	0
065[b]	10	**8**	3	5	0	**5**	0	0	0	0
066[b]	63	**11**	6	5	0	**5**	1	0	1	0

067[b]	12	**16**	13	3	0	**3**		0	0	0	0
068[b]	13	**24**	23	1	0	**1**		0	0	0	0
Arduino[a]	10	**8**	4	4	0	**4**		0	0	0	0
Boom Cards[a]	38	**19**	14	5	0	**5**		0	0	0	0
Code Combat (student)[a]	12	**10**	3	7	0	**7**		2	0	2	0
Code Combat (teacher)[a]	12	**10**	6	4	0	**4**		2	0	1	0
Code.org[a]	65	**21**	16	5	0	**5**		0	0	0	0
CodeHS[a]	31	**15**	10	5	0	**5**		1	0	1	0
Desmos[a]	43	**27**	24	3	0	**3**		0	0	0	0
Educreations[a]	10	**8**	3	5	0	**5**		0	0	0	0
Kami app[a]	27	**12**	6	6	0	**6**		0	0	0	0
Starfall[a]	34	**2**	1	1	0	**1**		0	0	0	0
Typing Club[a]	23	**13**	8	5	0	**5**		0	0	0	0
Tinkercad[a]	29	customDPA				**4**		0		0	0
080[b]	67	customDPA				**10**		2		1	0
081[b]	56	PrivPolicy customDPA				**7**		0		0	0
082[b]	86	PrivPolicy customDPA				**5**		0		0	0
Spotify[d]	9	PrivPolicy				**6**		1		2	2
084[b]	47	PrivPolicy				**6**		1		3	2
085[b]	18	PrivPolicy				**6**		4		3	1
086[b]	25	PrivPolicy				**5**		1		2	0
Scratch[d]	28	PrivPolicy				**11**		1		1	0
088[b]	92	Statewide Agreement				**11**		5		5	2**
Utah Aspire+	95	Statewide Agreement						0		0	0
Utah RISE	75	Statewide Agreement						0		0	0
091[b]	52	Statewide Agreement				**7**		1		1	0
092[b] (student account)	114	Statewide Agreement				**15**		1		4	0
092[b] (teacher account)	114	Statewide Agreement				**17**		1		4	0

Notes: the DPA column may include the name of another form of contract that the app falls under if no DPA is signed.
*Those apps with 0 (zero) data elements allowed per the DPA do have a signed DPA, but no data elements specified.
** In follow-up conversations, the vendor indicated that advertising is not present on student-facing sites and/or their education-specific offerings.
Superscript legend: a: Vendor chose to have their name published in the report; b: Vendor provided sufficient response via explanations, assurances, signing a new DPA, or making configuration changes and chose to be redacted; c: Vendor did not provide sufficient response; d: Vendor did not respond all, respond in time, or stopped responding.

There are several individual findings worth discussing in detail. First, several EdTech providers have been objectively verified to be honoring their legal and contractual obligations. Arduino, Boom Cards, Desmos, Kami App, Starfall, Typing Club, 067, 068, 082, Utah Aspire+, Utah RISE all appear to be collecting only the data necessary for their apps and are not sharing that data with any third parties. There are others like 080, 018, 086, and 091 that are sharing with third parties, but we have no evidence that those parties are not "subprocessors" that they are legally allowed to share data with. The State of Utah may consider requesting a list of these subprocessor third parties from these types of app vendors to confirm the legality of their data sharing.

Next, while there are bright spots in the results, the overall story appears that there are more apps in breach of their DPAs than not. Each of the apps listed in Column 4, "Collected but not allowed," with values greater than zero represents clear violations of contracts. In summary, in 44 of the 85 apps with SDPC-based DPAs (52 percent), EdTech apps collect at least one data element that is not contractually permitted. A few of these inconsistencies may be unintentional. For example, the company representative for an EdTech app may not have understood exactly what their app needed to collect when the DPA was signed and they erroneously selected the wrong data elements. It is also possible that updates to the app were made after the contract was signed. While this is still a violation, it does not necessarily indicate malicious intent (see Figure 6).

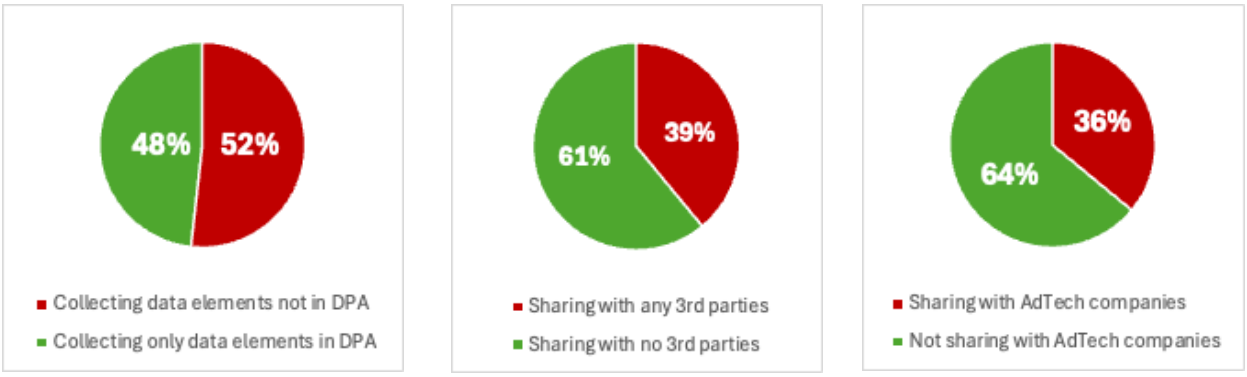

Figure 6. Summary of Network Traffic Testing Results

Eleven apps (13 percent) are also found to be sharing at least one data element that was not indicated in their DPA with a third party. 61 percent of apps are sharing data elements with third parties. And 36 percent are sharing data elements with advertisers—and a few of them are sharing with dozens of advertisers (005 = 32 advertisers; 026 = 54 advertisers; 041 = 33 advertisers).

In follow up conversations with EdTech vendors, most (20 out of 36, or 56%) indicated that targeted/behavioral advertising, or advertising generally, is not present in their student-facing applications or education-specific offerings. However, it is unclear whether schools were exclusively using the student-facing or education-specific applications, and we believe there is variance across vendors concerning whether most schools are using the "safe" student-facing or education-specific version versus the "unsafe" consumer-facing versions.

For example, we noticed that one vendor advertised an education-specific version of their application in a relatively small link in a non-central portion of their website while the more prominent version advertised is the commercial, non-education-specific version. This vendor did not offer the student-facing version on their website at all until they were pressed to explain the data sharing found in their more prominently

displayed app. Even though there is a version of that app that is safe for students to use, we see it as unlikely that all or possibly even a majority of schools are using the safe version at the time of this data collection.

On the other hand, we believe that many vendors were honest in their efforts to have LEAs only use the student-facing or education-specific version of their apps. We could not ascertain the degree of safe version usage in each of these scenarios. In summary, the results from this phase indicate what is *possible* and not necessarily what is *certainly* occurring in student app usage. Because we could not verify which version is being used across all Utah LEAs, we believed it fair to allow these vendors to have their names redacted from the report.

Related, seven of the vendors contacted indicated that their data handling practices, especially in regard to advertising, vary depending on whether the LEA is using the free or paid/premium version of their application. Given that most LEAs view a DPA as an indication that a vendor's product is safe to use, the USBE reviewer expressed concerns to these vendors that these distinctions were not clear enough in their DPAs. All of the vendors with DPAs were willing to clarify, in future iterations, that the DPA only applies to their paid/premium services, which will help provide clarity and reduce LEA app-vetting burden.

Next, while many data elements were shared with third parties, the most shared data element with advertising entities is a UUID that can be used for online profiling and behavioral advertising. This data element is not listed in any signed DPA contract as a permissible collection. EdTech vendors could have specified it in free text under the "Other" option. Some vendors may consider UUID to fall under the DPA entry "IP address of users, use of cookies, etc.," which is why they may not have specified it in "Other." Additionally, these unique user identifiers are expressly labeled as personal information in COPPA (1998, 16 CFR § 312.2). It is also important to note that many of the apps were also sharing data with known aggregator platforms, such as Microsoft, Google, Facebook, Twitter (X), and Amazon (see Appendix D for these details). These companies compile the data from EdTech apps. While we cannot verify what these companies are doing with the data we tracked, it is well-documented that these companies used such data in the past for behavioral advertising and marketing (Boerman et al., 2017).

Another interesting observation came from testing one app twice at two different periods of time several months apart. The data sharing behaviors of the app were very different at each testing. In the first test, the data collected was shared with nine third parties of which eight were advertising related entities. The second test indicated no data sharing whatsoever. There are multiple possible explanations for this. It could be that the EdTech vendor has permanently turned off all data sharing from their app. If that is the case, it was not due to any intervention on our part. It is also possible, and perhaps likely, that the app was simply not scheduled to share data during the second testing. Apps most commonly share data when an account is initially created and then reshare that data on some set schedule over time to keep the data "fresh." The implication is that although the presence of data sharing in a network traffic test indicates that data can be shared by the app, the lack of data sharing in a test does not indicate that data is never shared by the app.

Finally, not all data elements represent the same risk to students. A few elements are relatively benign, while others represent personally identifying information (e.g., name, email, address, phone number). Elements like gender, class schedule, teacher/counselor names, age, and ethnicity represent data that, when combined with other data, can be used to indirectly identify individual students. Elements like IP addresses and UUIDs represent data that can be used to generate an online profile that can be sold to aggregators or advertisers to target the student with customized ads. Prior research has revealed that children have been targeted with online advertising that is not age-appropriate (Burroughs, 2017) or could

be health-averse (Tan et al., 2018). We recommend that decision-makers also review the more detailed result tables below that outline exactly which data elements are being collected and shared by each tested app.

Apps for Further Investigation

There are several findings worth discussing that may warrant additional investigation by legal professionals. While some of the applications in this section are now deidentified, the USBE representative was able to communicate with them and can follow up. 085, 084, Scratch, and Spotify do not have a signed DPA. 084's privacy policy does state that they will use data for behavioral advertising, which was discovered and verified during our investigation. COPPA prohibits the use of behavioral advertising for children under the age of 13. Each of these apps was verified to be sending data to advertisers and/or aggregators while using accounts generated for children under the age of 13 years.

092 and 091 do not have signed DPAs, but both fall under a USBE contract. While we did not find evidence that they sent data to advertisers, they were sending data to aggregator platforms. The legality of this practice is somewhat less clear to us and may need to be reviewed by legal professionals. The following is the relevant wording we found in the USBE contract:

> *37.6.4. Contractor shall not use Data for any secondary use, including Targeted Advertising, except under Revised: 7-12-19- AMENDED 9/1/2020 6 the following conditions:*
>
> > *37.6.4.1. For adaptive learning or customized student learning purposes.*
> >
> > *37.6.4.2. To market an educational application or product to a parent or legal guardian of a student if Contractor did not use Data, shared by or collected per this Contract, to market the educational application or product.*
> >
> > *37.6.4.3. To use a recommendation engine to recommend to a student (i) content that relates to learning or employment, within the third-party contractor's application, if the recommendation is not motivated by payment or other consideration from another party; or (ii) services that relate to learning or employment, within the third-party contractor's application, if the recommendation is not motivated by payment or other consideration from another party;*
> >
> > *37.6.4.4. To respond to a student request for information or feedback, if the content of the response is not motivated by payment or other consideration from another party.*
> >
> > *37.6.4.5. To use Data to allow or improve operability and functionality of the third-party contractor's application.*

086 does not have a DPA or any other type of signed contract. Their privacy policy states that the username will be anonymized to all other users. We found evidence that the username is being shared with third parties. This may not be problematic if the username is anonymized, but we could not verify whether the username was the original or anonymized version.

Finally, it is important to remind the reader that the data collection on DPA data elements that were agreed to was completed in the summer of 2023. It is possible that certain updates or revisions have

been made since then, which could affect the accuracy of Table 3. The detailed results from each of the 100 app tests are included in Appendix D.

Transparency as an Effective Change Catalyst

The results above can be used to effect useful changes for the better.

Outside of this report, and separate from it, ISL performed two "responsible disclosures" of serious privacy risks for children as part of their non-profit work.

- A unique personal identifier for cross-site tracking was found in PBSkids.org. While PBS—as a nonprofit organization—is not obligated by COPPA, ISL raised the concern to several PBS executives. When no reply was received, ISL published a report (https://internetsafetylabs.org/blog/research/comscore-cross-site-tracker-found-in-pbskids-org/) exposing the situation. Within six weeks, PBSkids removed the problematic tracker from the site.
- CoolMathGames.com was observed to be sending traffic to dozens of advertising-related companies. Moreover, ISL testers found that the site performed location-based behavioral advertising. ISL notified CoolMath[4] in late 2023 of the COPPA-violating behavior on the site. Despite ISL's repeated attempts, no changes were made. In May 2024, ISL published the disclosure, https://internetsafetylabs.org/blog/research/isl-finds-location-based-advertising-on-kids-site-coolmathgames-com/, whereupon CoolMath proceeded to update the site, the site's privacy policy, and terms of service to indicate that CoolMathGames.com was *not* intended for children under the age of 13 years and that its other service, CoolMath4Kids.com, was the service intended for children under the age of 13 years. ISL recommends that no students use CoolMathGames.com due to the volume and nature of advertising. It further recommends that the USBE ensure that DPAs are in place for the use of any CoolMath offering.

Vendor Follow-up Details and Observations

As mentioned above, after the network traffic data was compiled, vendors were given an opportunity to respond to the results to refute, explain, or remediate the identified issues. If a vendor provided sufficient response to the requested actions, they were provided the option to redact their app/vendor name from the published report.

ISL provided raw data files to a representative from USBE's Data Privacy team who then used that data to compose letters to the vendors. For apps with DPAs, contact information was confirmed via an initial email to the email addresses in the most-recent, active DPAs. For apps without DPAs, contact information was found on app websites, through support channels, or statewide contract representatives. In cases where the vendor didn't respond to the initial request (either because of bad email addresses or turnover), the USBE representative then reached out to the contact information found in their privacy policies, resorting to support emails if that were also unsuccessful. Of the vendors emailed, eight did not respond at all; for some, contact was confirmed, but a formal response was not provided (detailed in Appendix D, as applicable). Only one vendor failed to provide a satisfactory response to the requested actions, which will be described below.

[4] We use "CoolMath" as a shorthand for CoolMath.com LLC, owned by Sandbox Group, which was the company that responded to our responsible disclosure.

Requested Actions

Vendors received four categories of requested actions:

Exhibit B Mismatch

As previously described, the Exhibit B in the DPA serves as a schedule of data for the vendor to indicate the student data that they will collect or process. In cases where vendors' data schedules did not align with ISL's results, the provided letter requested that they explain the discrepancy or sign a new DPA. 50 vendors received this as a requested item in their letter; of those, 31 signed–or committed to sign–a new DPA to address the discrepancies. As part of the back-and-forth correspondence, 13 vendors adequately explained the variances, which made signing a new DPA unnecessary. Primarily, these variances arose from the ISL researcher utilizing a commercial account for testing versus an account that would be licensed by a school or district. For example, a vendor may request a child's birthdate as a gate to their services to comply with COPPA, which may then prompt the child for their parents' contact information. In a school setting, COPPA is not relevant, and thus the vendor does not request these elements. These variances were subsequently removed from the app's result, both in Table 3 and the associated Appendix D entries. Five of the remaining vendors did not respond to the letter at all and one vendor, Loom, expressed that their new ownership disallows customer- and product-specific agreements, which resulted in the USBE representative considering their response insufficient.

Aggregators/Analytics

When ISL's entries denoted that a vendor utilized analytics/aggregator services (such as Google, Microsoft, or social media companies like X (Twitter), Facebook, or Pinterest), the USBE representative requested that the vendor provide assurances or evidence that these services are not resulting in noncompliant re-disclosure of student data and/or targeted or behavioral advertising. Many vendors utilize Google Analytics or Microsoft to improve their services, which is allowable under FERPA and the DPA's provisions, as long as the vendor is handling data with equal stringency as the primary vendor. To that end, these services can be configured to provide anonymous analytics; however, both Google and Microsoft's analytics services can be utilized to facilitate targeted advertising, either intentionally or unintentionally. 54 vendors received letters listing "aggregators/analytics" as an item requiring response. Of those 54, six vendors modified the identified misconfigurations, which did appear to be unintentional or remnants from upgrading analytics versions; the remaining vendors provided assurances and/or evidence and screenshots that their analytics were anonymous or only present on teacher-facing pages.

Social Media

Social media integrations were occasionally listed by ISL as both aggregators and as advertising-related entities, depending on their review. Social media integrations may be used for the purposes of sharing pages and content or linking accounts for authentication; for example, signing into a website using one's Facebook credentials. In some cases, utilizing social media for account authentication can be benign, but the convenience does carry the risk of tracking users for the purposes of targeted advertising. This authentication scheme is uncommon in schools, especially for students, with the exception of utilizing Google Workspace for Education for authentication. Often, website builders may rely on social media plugins, which place buttons on pages to easily share content to social media or link to the website owner's own social media pages. Occasionally, depending on the plugin, these integrations can result in third-party

cookies being placed into a user's browser, which facilitate targeted/behavioral advertising and building profiles of a user's activities across other websites and/or their interests and demographics. As website owners may not be aware of the ramifications of these social media integrations and/or plugins, the USBE reviewer treated these as a separate category of requested action and response, where applicable. One common finding during review was that websites that offer both commercial and educational services may remove any social media integrations once a student is logged in, but the cookies were still being placed in the user's browser when they navigated to the main website to login. While nearly all websites now offer the user a choice to block third-party cookies, the USBE Data Privacy teams feels that the burden should not fall onto students or LEAs who expect thorough data privacy from their contracted service providers. Nearly all of the vendors to whom the USBE reviewer expressed this concern were willing to consider ways of mitigating the issue. 11 vendors received the social media item as a requested action and response. Three vendors made changes to remove this traffic from student-facing websites. Four vendors stated that this traffic isn't present when a student logs in. Three vendors didn't respond to their requests, and one stated that the website was not intended for students.

Advertising-Related Entities

As previously noted, utilizing student data for targeted/behavioral advertising is expressly prohibited by FERPA, COPPA, Utah state law, and thus the provisions of the DPA. 28 vendors received this item as a requested action, prompting them to either explain or remediate the identified traffic. In the letters provided to the vendors, the USBE reviewer included screenshots–where applicable–of traffic that appeared to be problematic and/or third-party cookies or domains that were known to be related to advertising and marketing. As previously noted, this network traffic was occasionally related to social media integration or the result of misconfigured analytics, such as Google Ads or Doubleclick traffic. Additionally, video embeds could be a source of advertising activity, as embedding videos from certain sites can result in advertising-related cookies by default (though this behavior can be mitigated). A common response by vendors was that their paid services do not utilize advertising; however, this distinction was often not made readily apparent as part of the DPA process. As previously noted, vendors that were asked to be more specific about their services in their future DPAs were all willing to do so.

Of the 28 vendors contacted, seven of them had free or paid services that behaved differently in terms of advertising. Similarly, six vendors indicated that their standard, commercially available services differ from their education-specific offerings in terms of advertising (and presumably other forms of data processing); one of these vendors made additional configuration changes to their education-centric website to address the identified network traffic. Two of the vendors explained that their services are intended for educators and are not directly used by students; one of those vendors mitigated the identified behavior, regardless. Two vendors provided screenshots and assurances that advertising and/or analytics are not present when a student signs in. One vendor adequately explained the nature of the identified advertising and the purpose of its anonymous usage. One vendor's privacy policy openly states that they allow targeted advertising, and thus student data should not be provided to that app (most LEAs note this on their MDDs and indicate that the app is for teacher use only). Four vendors did not respond to the letter.

Seven vendors in total modified, or had already modified, their website to address the requested actions, which typically involved changing analytics, video embedding settings, or removing tracking pixels. In the cases where vendors modified their website, the USBE reviewer does feel that they were being honest in their report that the behavior was not malicious or intentional; however, these findings do support the benefit of auditing and monitoring any services that receive student data to ensure that these issues are addressed in a timely manner and that vendors can be held accountable when student data is mishandled.

Vendor Follow Up Recommendations and Summary

The USBE representative noted several key findings as part of the back and forth follow up with vendors resulting from this investigation. Nearly all the vendors were keen to work with the USBE representative to address or respond to the findings. While some vendors were initially defensive or quick to use legal language, their demeanor softened once they realized that the USBE representative was interested in finding collaborative solutions toward a shared goal.

While most vendors were eager and collaborative in their responses, the USBE representative encountered notable exceptions to that trend. Some less-than-desirable responses came from apps that may be used in an educational setting but are primarily standard, commercial products. Products specifically designed for education were less likely to need background information on student data privacy laws and regulations, or the provisions of the DPA and, as a result, were more likely to be handling student data seemingly more adeptly and safely. The USBE Data Privacy team recommends that greater care should be taken when schools choose to use websites and applications that are not primarily designed for student or educational use.

Furthermore, the tendency for websites and technology to be merged or acquired represents a risk to student data privacy. There is demonstrated risk that new owners or parent companies may not understand their obligations surrounding student data privacy, or they may not honor existing agreements, data ownership, or data retention schedules.

An additional observation is that thorough completion of the Exhibit B in the DPA deserves greater attention and improvement. Some vendors were unaware that the schedule of data should include data elements that they "process"—meaning data that is created and associated to the student, provided by the student directly, or created as part of a student's use of the service. It should be noted that older versions of the DPA defined student data to only be data provided directly by an LEA, thus this behavior could be a holdover from that previous definition. Additionally, as evidenced by the Appendix D entries, vendors occasionally appear to mark more data elements than they require, which may be attributed to a lack of clear definitions. As noted in commentary surrounding UUIDs, the DPA does not provide many specific options for a vendor to indicate the exact metadata they may process, which then requires the vendor to provide that data element in free-text form. The USBE representative notes that while many vendors are seemingly not thorough enough in their Exhibit B entries, some vendors, such as Boom Cards, deserve recognition for utilizing the Exhibit B as an impressive exercise in transparency and rigor.

Finally, while the existing legislation and compliance requirements for student data privacy are robust, the process for rigorously complying with those requirements is often difficult–for both the LEA and vendors, alike. This exercise demonstrates that greater collaboration, auditing, monitoring, training, and enforcement can help to drive real, measurable change–especially when all parties view each other as partners in the critical goal of protecting our students and their data.

Four Vendor Response Categories Affecting Redaction

As previously described, a vendor's name appearing in this report was based on their response after receiving their results. We describe four types of responses received in greater detail below:

Category A: Vendor Chose to Remain Named

Some vendors when offered optional redaction chose to remain named in the published report. Most of these vendors did not receive any actionable findings or requested actions. Other vendors were presented with minor Exhibit B mismatches, which were sufficiently explained, and some were asked to provide assurances in their safe usage of analytics tools, which they readily provided. Vendors in this category, who decided to remain named, were pleased to feel recognized for their efforts in safeguarding data. Some vendors expressed a desire to post their results publicly on their website.

This positive experience suggests that collaborative audits can be an avenue for recognizing good work and strong partnerships, which may then incentivize and positively reinforce other vendors.

Category B: Vendor Opted for Redaction After Adequate Response

Vendors who fall into this category opted for redaction after satisfactorily responding to the requested actions. Vendors signed new DPAs where appropriate or modified technical elements of their app and/or data collection and processing. Many of these vendors did not appear to feel threatened by the results of this report and were willing to collaborate. We classify this as a desirable response even though inconsistencies were found because they were simply mistakes or misunderstandings made by well-intentioned companies. In these cases, we caution against any initial feelings of outrage when initial inconsistencies are found because beneficial relationships of trust can be built with these types of vendors. Given that research has shown that EdTech usage in schools does have an overall positive effect on learning (Earle, 2002; Grayson, 1972; Honey et al., 2000), we do not want to limit its usage in the classroom by promoting public outcry.

Another way that some vendors addressed their inconsistencies was by stating that they have a separate version of their app that is designed for education or is “student-facing,” as referred to earlier in the report. This was somewhat of a gray area of response because although we may have personal feelings about which vendors were being genuine and which were not, we could not objectively validate their claims since these student-facing versions were not available to us at the time of testing. It is likely that some were sincere and some were not. We believe it would be useful for the State of Utah to provide the USBE Data Privacy team (or similar) the resources necessary to build and maintain relationships with EdTech vendors so that the State can perform their own network traffic testing of these apps on an ongoing basis.

Category C: Vendor Remained Named Due to Inadequate Response

Only one vendor, Loom, is named in the report under this designation. Loom was acquired by Atlassian. The USBE representative struggled finding someone at Atlassian who could answer questions related to their app’s results, which was worsened by a general lack of knowledge from their staff surrounding student data privacy. This process resulted in numerous back-and-forth messages with intermediaries before a meeting could be scheduled with their privacy team. Because DPAs are signed with an originating LEA, which can then be subscribed by others, Atlassian representatives did not understand that USBE’s request was broader than one client. Atlassian claimed that they had no record of the originating LEA utilizing their services, which is worrisome as the originating LEA was a Loom customer. Eventually, the USBE representative was able to meet with their privacy team where the extensive breadth of student data privacy considerations could be explained. While the meeting was productive and friendly, the representative noted that Atlassian has a policy against allowing customer paper or differentiating data handling by client, meaning that Atlassian would presumably not be willing to sign a DPA for Loom. In similar cases, USBE

reviews a company's DPA to determine if their data handling complies with student data privacy laws; thus, there may still be a route for LEAs to continue to use Loom. While the Atlassian representative did appear willing to have further discussions, because they were unwilling to sign a new DPA, their response was considered insufficient.

Notably, this scenario is emblematic of the issues that can arise when company ownership changes hands. We are uncertain if Loom contacted LEAs at the time of acquisition to describe how they would meet their student data privacy obligations.

Category D: Vendor Remain Named Due to Nonresponse

Finally, some vendors simply did not respond to the USBE Data Privacy team's notifications. In these cases, we recommend that LEAs consider discontinuing their usage of these apps until the vendors are willing to address their inconsistencies. While the USBE representative did attempt multiple avenues of contact, there may be legitimate reasons for the lack of response, such as inactive email addresses, outdated privacy policy contact information, turnover, or unclear support channel nuances. There was no obvious trend for vendor unresponsiveness; for example, some of the vendors who failed to respond had minor findings in their reports that may have been easily remedied or explained.

We caution against drawing negative conclusions about these vendors before understanding the root cause of their unresponsiveness and hope that they will consider reaching out to USBE after publication.

Further Discussion and Potential Recommendations

The State of Utah has a good process in place to gain privacy assurances before apps are adopted. We reviewed these processes and the training given to LEAs and found that the processes are reasonably followed throughout the state. Indeed, based on our experience, the state of Utah may be "ahead of the curve" relative to other states when it comes to its EdTech data privacy standards and practices—particularly regarding the use of DPA contracts and the level of detail regarding data elements allowed by each contractor.

We wish to point out two other positive structures already in place that are beneficial to student privacy. First, this project was initiated by the USBE. Even though there is always a possibility that even a small amount of negative results from investigations like this one can be damaging, this group put the best interests of students first and approved/funded this project with the earnest intention of maintaining student privacy. Second, the USBE Data Privacy team was very effective in supporting and aiding this project. Their efforts to train LEAs on data privacy regulation and protective practices for students appear very effective. We could not have achieved the results in this report without their help.

This project provided objective data for the USBE Data Privacy team to engage in meaningful discussions with EdTech vendors to seek clarification and explanation of the observed behaviors leading to a smarter "trust, but verify" approach. We applaud this team who completed the work required to inform each vendor of their network traffic results and achieve reconciliation. We believe this team has developed an exemplary process to achieve greater congruence between DPAs and "results in practice." In fact, this reconciliation process could provide an example to other states who are similarly interested in maintaining student privacy. In essence, this process gave vendors an opportunity to "show their true colors" in how they responded when inconsistencies were discovered.

Importantly, we reiterate that the potential privacy violations discovered from this research should not be attributed to, or blamed on, teachers, administrators, or LEA-level data privacy managers. They cannot be expected to perform their own network traffic testing. While network traffic testing has become more accessible, it is still outside the bounds of what should be expected from these decision makers. Their responsibility is to review what EdTech vendors have agreed to in signed contracts, DPAs, or their public declarations in privacy policies. No EdTech app within Utah schools should be used without 1) reviewing existing DPAs signed by other LEAs, 2) determining whether there exists, and identifying, the “safe” student-facing or education-specific versions of an app (which may involve paid licensing), and 3) understanding the implication of this report that excessive data collection and sharing is common among most EdTech vendors. It may be very convenient to try out off-the-shelf apps in a classroom without fully understanding the privacy implications. In these cases, teachers and decision-makers could use resources such as the appmicroscope.org database to make informed decisions.

Additionally, it is important for LEAs to ensure that EdTech vendor representatives who fill out DPAs take care to complete Exhibit B accurately. Omitting data elements that will be collected or processed is a violation of the agreement and causes LEAs to make decisions that are not fully informed. Similarly, marking excessive data elements that will not be collected may cause decision-makers to avoid using EdTech that could be very useful in the classroom. In summary, LEA data privacy managers should ensure that vendors are careful to mark only the appropriate data elements in Exhibit B. Perhaps, informing the EdTech vendors before they sign a DPA that their products will be fully tested over time will encourage greater transparency upfront.

Concerning Exhibit B of DPAs, it is important to reconcile misunderstandings or misalignment around the collection of UUIDs. As mentioned earlier, UUIDs can be utilized for benign technical reasons, but UUIDs can also be generated to create identity graphs, which are an aggregation of everyone's usage behaviors across all apps and websites. Data aggregators and brokers benefit most from UUID tracking, as they use it for behavioral marketing—something the SDPA restricts for all students and COPPA restricts for children under 13. UUID generation and usage includes the following steps. First, an app or website collects data that will uniquely identify users like their IP address, device ID, login credentials, or existing browser cookies. Next, the app or website checks a database of identity graphs to see if this user already has a profile. This database could belong to the first-party app or website, but it could also belong to much larger third-party data brokers and aggregators. If a match is found, then the existing UUID is stored in the user’s cache so that the first-party app/website can more quickly match their future online behavior with the rest of their profile. If no match is found, then a new UUID is created for the individual and also similarly stored in the user's cache. To be clear, the presence of the UUID element in a vendor’s results does not necessarily implicate them in this behavior. UUIDs have many safe and reasonable operational use-cases; however, as it is an element that can be misused and mishandled, we feel that it deserves greater scrutiny.

The issue is that standard DPAs do not clearly account for UUIDs in Exhibit B as there is not a clear option to indicate that UUIDs are being collected/generated. Many of the apps were found sending UUIDs without ever explicitly indicating so in their Exhibit B. This could be a result of there being no explicit box on that form marked as “UUID”. While it could be argued that vendors should have indicated UUIDs using the “Other” box, they could at least mark “IP address of users, use of cookies, etc.” Of those who were found to be transmitting UUIDs, some had marked “IP address of users, use of cookies, etc.” on their DPA (which could be argued is a partial fulfillment of disclosing their collection of UUIDs) whereas others did not mark it in any way. The optimal solution to this issue would be to modify future iterations of the DPA to provide greater in-built specificity surrounding metadata, thus negating the need for a vendor to list these items in free text.

We recommend continuing the network traffic testing of apps. This form of data investigation has shown promise in prior research as a method for initiating positive changes toward student data privacy. As this practice becomes standard in the EdTech space, providers will become more privacy-conscious and make fewer mistakes in their data collection and sharing practices, thereby leading to more robust student data privacy management. In addition, those who intentionally violate DPAs will be more hesitant, knowing that their practices are more likely to become transparent. Most importantly, network traffic testing will allow the USBE Data Privacy team to continue building relationships of trust with ethical EdTech providers while weeding out those that violate agreements. We invite state regulators and budget-allocators to consider the funding requirements of providing this testing and encourage them to recognize the value in this work.

We recommend that EdTech apps that have not yet been investigated by the state of Utah be reviewed at https://appmicroscope.org/. This database provides at least a snapshot at some point in time of the network traffic-tested data collection and sharing practices of EdTech apps. This database is not complete and does not include every version of every EdTech app. Furthermore, the actual data collection and sharing practices of EdTech providers will change over time. This database provides a useful starting point until the state can perform its own investigation of apps.

Acknowledgments

We sincerely thank the USBE for providing grant funding for this project. We appreciate that USBE has prioritized student data privacy in the state. We also thank the USBE Student Data Privacy team for their review of the project deliverables and report.

References

Akar, E., & Nasir, V. A. (2015). A review of literature on consumers' online purchase intentions. Journal of Customer Behaviour, 14(3), 215-233.

Boerman, S. C., Krulkemeler, S., & Borgesius, F. J. Z. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. Journal of Advertising, 46(3), 363-376.

Burroughs, B. (2017). YouTube kids: The app economy and mobile parenting. Social media+ society, 3(2), 2056305117707189.

Carlsson, R., Heino, T., Koivunen, L., Rauti, S., & Leppänen, V. (2022). Where does your data go? comparing network traffic and privacy policies of public sector mobile applications. World Conference on Information Systems and Technologies,

COPPA. (1998). Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Dalsen, W. (2009). Civil remedies for invasions of privacy: A perspective on software vendors and intrusion upon seclusion. Wis. L. REv., 1059.

Earle, R. S. (2002). The integration of instructional technology into public education: Promises and challenges. Educational technology, 42(1), 5-13.

FERPA. (1974). Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FTC. (2013). Complying with COPPA: Frequently Asked Questions. Retrieved July 2nd, 2024, from https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

FTC. (2021). A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority. Retrieved June 30, 2024, from https://www.ftc.gov/about-ftc/mission/enforcement-authority

GrandViewResearch.com. (2023). Education Technology Market Size, Share & Trends Analysis Report By Sector (Preschool, K-12, Higher Education), By End-user (Business, Consumer), By Type, By Deployment, By Region, And Segment Forecasts, 2023 - 2030. Retrieved September 18, 2023, from https://www.grandviewresearch.com/industry-analysis/education-technology-market

Grayson, L. P. (1972). Costs, Benefits, Effectiveness: Challenge to Educational Technology: Problems and perspectives on analyses of costs, benefits, and effectiveness are discussed. Science, 175(4027), 1216-1222.

Grundy, Q., Chiu, K., Held, F., Continella, A., Bero, L., & Holz, R. (2019). Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ, 364.

HB358. (2016). H.B. 358 Student Privacy Amendments. Retrieved June 26, 2024, from https://le.utah.gov/~2016/bills/static/HB0358.html

Honey, M., Culp, K. M., & Carrigg, F. (2000). Perspectives on technology and education research: Lessons from the past and present. Journal of educational computing research, 23(1), 5-14.

iKeepSafe.org. (2024). The Certification Process; Understand the process and what vendors get from the subscription. Retrieved June 3rd from https://ikeepsafe.org/our-process/

InternetSafetyLabs.org. (2023). 2022 US K12 EdTech Benchmark. Retrieved Sep 18th, 2023, from https://internetsafetylabs.org/resources/reports/2022-us-k12-edtech-benchmark/

Jibb, L., Amoako, E., Heisey, M., Ren, L., & Grundy, Q. (2022). Data handling practices and commercial features of apps related to children: a scoping review of content analyses. Archives of disease in childhood, 107(7), 665-673.

Joshi, M., & Hadi, T. H. (2015). A review of network traffic analysis and prediction techniques. arXiv preprint arXiv:1507.05722.

Kemp, K. (2020). Concealed data practices and competition law: why privacy matters. European Competition Journal, 16(2-3), 628-672.

Marshall, R., Pardo, A., Smith, D., & Watson, T. (2022). Implementing next generation privacy and ethics research in education technology. British Journal of Educational Technology, 53(4), 737-755.

McDonald, N., & Forte, A. (2022). Privacy and vulnerable populations. In Modern socio-technical perspectives on privacy (pp. 337-363). Springer International Publishing Cham.

Morehouse, K. N., Kurdi, B., & Nosek, B. A. (2024). Responsible data sharing: Identifying and remedying possible re-identification of human participants. American Psychologist.

Pimienta, J., Brandt, J., Bethe, T., Holz, R., Continella, A., Jibb, L., & Grundy, Q. (2023). Mobile apps and children's privacy: a traffic analysis of data sharing practices among children's mobile iOS apps. Archives of disease in childhood, 108(11), 943-945.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company.

StudentPrivacyPledge.org. (2020a). K-12 School Service Provider Pledge to Safeguard Student Privacy 2020. Retrieved June 3rd from https://studentprivacypledge.org/privacy-pledge-2-0/

StudentPrivacyPledge.org. (2020b). Student Privacy Pledge Guidelines: Guidelines & FAQs. Retrieved June 30, 2024, from https://studentprivacypledge.org/faqs/

Sweeney, L. (2000). Simple demographics often identify people uniquely. Health (San Francisco), 671(2000), 1-34.

Tan, L., Ng, S. H., Omar, A., & Karupaiah, T. (2018). What's on YouTube? A case study on food and beverage advertising in videos targeted at children on social media. Childhood Obesity, 14(5), 280-290.

Taylor, V. F., Spolaor, R., Conti, M., & Martinovic, I. (2017). Robust smartphone app identification via encrypted network traffic analysis. IEEE Transactions on Information Forensics and Security, 13(1), 63-78.

UCPA. (2023). Utah Consumer Privacy Act (UCPA), Utah Code §§ 13-61-101 et seq. https://dcp.utah.gov/ucpa/

van Dam, J.-W., & Van De Velden, M. (2015). Online profiling and clustering of Facebook users. Decision Support Systems, 70, 60-72.

Yacobson, E., Fuhrman, O., Hershkovitz, S., & Alexandron, G. (2021). De-identification is Insufficient to Protect Student Privacy, or–What Can a Field Trip Reveal? Journal of Learning Analytics, 8(2), 83-92.

Appendix A – Glossary

Aggregator Platform

ISL has identified 7 Platforms that are considered very high risk when they are in possession of personal data. These platforms include Adobe, Amazon, Apple, Facebook, Google, Microsoft, and Twitter.

Cross-Site Tracker

A piece of code which is used to identify where a user has visited previously on the internet. Usually coupled with a unique user identifier (UUID) cookie to tie a user to a particular web-browsing history.

Cookies

Small blocks of data written to a user's computer when browsing websites. Cookies can be used to facilitate necessary website/app functionality, but cookies can also be used to track a user's web browsing activity for the purposes of targeted or behavioral advertising.

LEA Expected Data Elements

Data elements agreed to by the LEA in the contract with the EdTech company.

Local Education Agency (LEA)

"Local educational agency or LEA means a public board of education or other public authority legally constituted within a State for either administrative control or direction of, or to perform a service function for, public elementary schools or secondary schools in a city, county, township, school district, or other political subdivision of a State, or for a combination of school districts or counties as are recognized in a State as an administrative agency for its public elementary schools or secondary schools." https://sites.ed.gov/idea/regs/c/a/303.23

Personally Identifiable Information

Per Utah State Legislation 53E-9-301 (15a-b): Student Data Protection.

Personally-identifying information includes:

(i) a student's first and last name;
(ii) the first and last name of a student's family member;
(iii) a student's or a student's family's home or physical address;
(iv) a student's email address or other online contact information;
(v) a student's telephone number;
(vi) a student's social security number;
(vii) a student's biometric identifier;
(viii) a student's health or disability data;
(ix) a student's education entity student identification number;
(x) a student's social media username and password or alias;

(xi) if associated with personally identifiable student data, the student's persistent identifier, including:
  (A) a customer number held in a cookie; or
  (B) a processor serial number;

(xii) a combination of a student's last name or photograph with other information that together permits a person to contact the student online;

(xiii) information about a student or a student's family that a person collects online and combines with other personally identifiable student data to identify the student; and

(xiv) information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

Student Data Privacy Agreements (DPA)

A standard contract used by LEAs to allow the adoption of EdTech apps in schools.

Student Data Privacy Consortium (SDPC)

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

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

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

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

Targeted/Behavioral Advertising

Targeted advertising is the practice of delivering ads to consumers based on specific traits such as demographics, interests, location, or behaviors. The goal is to improve ad relevance and increase the likelihood of engagement or conversion. Targeting dimensions may include data points like age, gender, income, geolocation (e.g. city, ZIP code), device type (e.g. mobile vs desktop), interests (e.g. sports, parenting), and past purchases or browsing history.

Behavioral advertising is a subset of targeted advertising that relies specifically on tracking users' online behavior over time—such as websites visited, searches made, videos watched or clicks—to infer interests and serve personalized ads. It often involves tracking cookies or browser fingerprinting, building profiles of users' habits, cross-site tracking and retargeting.

Unique User Identifier (UUID)

Unique User Identifier is a tracker which contains sufficient entropy and length to be unique to each person in the world. These trackers are often used to track user movement across the internet to build

advertising profiles, though they may also be created and used for benign website/app management and database functionalities.

Appendix B – Testing Methodology

For each web service, ISL first tested the home page. From there, ISL next tested either account creation, logging in, or just directly using the service for sites that don't require a log in.

For sites that require or allow account creation:

- If the sites required LEA-provided credentials, ISL used credentials provided by the LEA(s).
- If the service allowed for account creation, an account was created to mimic a child student user under 13 years old.

Data was collected on what personally identifiable information (PII) was needed to create an account, and what information was needed to be provided by/about a parent.

General Testing

Web service testing began with recording all network traffic while using the site. Then ISL analyzed web traffic to and from the web service. This included:

- Identifying all the data written to local storage (such as cookies, for example) during the session.
- Identification of the companies that wrote to local storage, the duration of the cookie/data, and its general purpose.
- Searching network traffic to confirm what code wrote to local storage and where the data was being sent/shared.
- Analyzing domains and subdomains to understand the company who owned the domain/subdomain and what function it served.
- For each network call, parsing the request and response. By looking at what data was sent to which servers in HTTP requests, we were able to identify which data elements were being sent to first parties and which were being sent to third parties.

Web services were tested for approximately 15 minutes and all functionality (each user interface path) was tested. Where available, assignments/tests/study quizzes were performed, and user profiles were edited. During this test, data was collected on what data elements were being entered and/or edited by the user.

Unable to Test

Certain conditions prevented ISL from readily capturing network data.

- Services that require a proprietary secure browser encrypt the traffic between the user and the server to which they are connecting. Because of this encryption, it is not possible to view the traffic in a meaningful way. The only legal way to view the data would require an agreement from the service owner, and falls into the category of "Penetration Testing" or "Ethical Hacking."

Appendix C – Personal Data Relevant to EdTech

Based on our review of Utah's data privacy agreements and the SDPC registry, Table C1 below summarizes the list of relevant data elements. The Internet network traffic investigation revealed a few other data elements that were also relevant including *teacher information* and *unique user identifiers* for tracking online profiles. Certainly, there may be more data types that could be added or removed from this list in the future.

Table C1. List of 79 Data Elements Considered in Data Privacy Agreements

entity	Name	category
student	email	contact
student	phone	contact
student	biliteracy level	demographics
student	birth date	demographics
student	birth place	demographics
student	disability information	demographics
student	English language learner information	demographics
student	ethnicity	demographics
student	foreign exchange information	demographics
student	gender	demographics
student	grade level	demographics
student	immigrant refugee status	demographics
student	living situations homeless foster care	demographics
student	migrant information	demographics
student	native English speaker	demographics
student	other demographic information	demographics
student	special education disability information	demographics
student	specialized education services	demographics
student	after school participation program	engagement
student	attendance information	engagement
student	career and technical education participation	engagement
student	dual language immersion info	engagement
student	extracurricular activities	engagement
student	individualized career plan information	engagement
student	title I program participation	engagement
student	course data	enrollment
student	homeroom	enrollment
student	school enrollment	enrollment
student	specific curriculum programs	enrollment

student	teacher counselor names	enrollment
student	economic status	financial
student	fee information	financial
student	income status	financial
student	intergenerational poverty grant participation	financial
student	app assigned ID number	identifier
student	app passwords	identifier
student	app username	identifier
student	images	identifier
student	name	identifier
student	other indicator information	identifier
student	state ID number SSID	identifier
student	address	location
student	bus assignment	location
student	bus card ID number	location
student	IP addresses	location
student	other transportation data	location
student	pick up drop off location	location
student	medical health information	medical
student	meta data on user interaction with application	other
student	online communications	other
student	other	other
student	web browsing history	other
student	youth in custody program information	other
student	assessment results	performance
student	assignment scores	performance
student	conduct behavior discipline incident information	performance
student	course grades	performance
student	generated content	performance
student	gifted indicator	performance
student	graduation completion info	performance
student	honors awards recognitions	performance
student	in-application performance	performance
student	literacy level intervention	performance
student	observation data	performance
student	video or voice recordings	performance
student	NCLB school choice	preferences
student	NCLB supplementary services received	preferences
student	survey results	preferences
parents	email	contact

parents	phone	contact
parents	ID number	identifier
parents	name	identifier
parents	address	location
parents	military status	other
school	21st century community learning center grant (21 CCLC)	school data
school	local ID number	school data
school	location	school data
school	region	school data
school	type	school data

Sub-totals	
Student elements	68
Parent elements	6
School elements	5
Total:	79

Appendix D – Detailed App Testing Results

These indicate data elements that are being collected by the provider, but are not specified in any data privacy agreement we could find

Advertising entities are not allowed in any DPA

001[b] (Teacher)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	x
Student app username		x	x
Student assessment results		x	x
Student course grades		x	x
Student birthdate		x	x
Student ethnicity/race		x	x
Student gender	x	x	x
Student generated content		x	x
Student grade level	x	x	x
Student, other*		x	x
Student in-app performance		x	x
Student income status		x	x
Student IP address	x	x	
Student name	x	x	x
Student language information		x	x
Student school enrollment		x	x
Student specialized education services (gifted indicator)		x	x
Student teacher/counselor names	x	x	x
Unique user identifier	x	x	x
Metadata on user interactions	x		
Student assessment observation data	x		

Additional Details	
LEAs using this app	14
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

002[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student enrollment, other**		x	
Student app password		x	
Student app username		x	
Student email		x	
Student IP address		x	
Student name	x	x	
Unique user identifier		x	x
Student grade level	x		
Student homeroom	x		
Student teacher names	x		
Student local ID	x		
Parent/guardian email	x		

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	3*
Aggregator platforms receiving data	Amazon, Google

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.
**Free-text data element description removed to maintain vendor confidentiality.

Loom[c]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	
Student app username		x	
Student email		x	
Student images		x	
Student IP address	x	x	
Student name		x	

Additional Details	
LEAs using this app	0
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: Utah DPA V2: https://sdpc.a4l.org/agreements/SIGNED - LOOM_UT-DPA-V2_w_Exhibiit-E_1.doc.pdf
c: Vendor name not redacted due to inadequate response.
Loom was acquired; the new owner has a policy against signing customer paper, which prevents an LEA from signing a new DPA with them. The USBE team will need to review the new owner's custom DPA to determine if it aligns with state student data privacy laws.

Replit[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	
Student email		x	x
Student IP address		x	
Student name		x	
Unique user identifier		x	x

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	1
Aggregator platforms receiving data	Google

Notes: Exhibit B is blank.
Utah DPA V2: https://sdpc.a4l.org/agreements/UT_replit_with_exhibit E.pdf
d: Vendor name not redacted due to nonresponse. USBE attempted to contact Replit through the email listed on their DPA and their support channels but never received a response.

005[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student IP address	x	x	x
Student user interaction data		x	x
Student app password		x	
Student app username		x	
Student address (city and state)		x	
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	15
Number of 3rd parties receiving data	34
Number of advertising related entities receiving data	32*
Aggregator platforms receiving data	Google

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

006[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent email		x	
Parent name		x	
Student app password	x	x	
Student app username	x	x	
Student birthdate		x	
Student email		x	
Student generated content	x	x	
Student name	x	x	
Student course grades	x		
Unique user identifier	x	x	x
Student IP address, etc.	x		
Metadata on user interaction with application	x		
Other assessment data**	x		
Other assessment data**	x		
Student teacher names	x		
Other**	x		
Other**	x		
Other**	x		

Additional Details	
LEAs using this app	32
Number of 3rd parties receiving data	19
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Google

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor corrected the identified misconfigurations in their analytics.
**Free-text data element description removed to maintain vendor confidentiality.

Vocabulary.com[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent/guardian email		x	
Student app password	x	x	
Student app username	x	x	
Student birthdate		x	
Student grade level		x	
Student in-app performance	x	x	
Student IP address	x	x	
Student address (city, state, country, zip code)		x	
Student app assigned ID number	x		
Student email	x		
Student name	x		
Student teacher names	x		
Metadata on user interaction	x		
School enrollment	x	x	
Student state ID number (SSID)	x		
Student local ID number	x		

Additional Details	
LEAs using this app	15
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/2024-09-11_6583_11685_signed_agreement_file.pdf
d: Vendor name not redacted due to nonresponse. USBE reached out to the email in the DPA and support channels but never received a response.

008[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent/Guardian address		x	
Parent/Guardian email (Optional)	x	x	
Parent/Guardian first and/or last name (Optional)	x	x	
Student enrollment, other*		x	
Student app password		x	
Student app username	x	x	
Student birthdate		x	
Student email	x	x	
Student gender	x	x	
Student grade level	x	x	
Student year of graduation	x	x	
Student IP address	x	x	
Student name	x	x	
Student phone	x	x	
Student address	x	x	
Student scheduled courses*	x		
Student English language learner info	x		
Student ethnicity	x		
Student low income status	x		
Student IP address	x		
School local ID number (Optional)	x		
Metadata on user interaction	x		
Student language information	x		
Student school enrollment	x		
Student teacher/counselor names*	x		

Additional Details	
LEAs using this app	20
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: Vendor Specific Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

009[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	
Student app username		x	
Student email		x	
Student IP address		x	

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: DPA indicates no student data collected.
Vendor Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

010[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	
Student app username		x	
Student assessment, other*	x	x	
Student demographics, other*	x		
Student school enrollment	x		
Parent/guardian email (optional)	x	x	
Parent/guardian ID number (optional)	x		
Parent/guardian first and/or last name	x		
Student teacher names	x		
Student email	x	x	
Student grade level	x	x	
Student in-app performance		x	
School local ID number		x	
Student IP address	x	x	
Metadata on user interaction	x		
Student name	x	x	

Additional Details	
LEAs using this app	56
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

011[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student IP address		x	x
Student name		x	
Unique user identifier		x	x

Additional Details	
LEAs using this app	18
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: Exhibit B is blank.
Utah DPA V2
b: Vendor provided sufficient response and requested redaction.

Flip

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	
Student app username		x	
Student birthdate		x	
Student email	x	x	x
Unique user identifier	x	x	x
Student generated content	x		
Student IP address	x		
Metadata on user interactions	x		
Metadata, other: device OS, browser OS, anonymous diagnostic data	x		
Student name	x		

Additional Details	
LEAs using this app	37
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google, Microsoft

Notes: Application was purchased by Microsoft and since shutdown.
Previous NDPA-V1: https://sdpc.a4l.org/agreements/Flipgrid OPA DPA Signed.pdf

013[b] (student account)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	
Student IP address	x	x	
Student in-app performance		x	
Meta data on user interaction		x	
Student name	x	x	

Additional Details	
LEAs using this app	15
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: DPA indicates that the app doesn't need to collect identifiable data. Utah DPA V2 b: Vendor provided sufficient response and requested redaction.

013[b] (teacher account)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student in-app performance		x	
Student name	x	x	
Student IP address	x		

Additional Details	
LEAs using this app	15
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: DPA indicates that the app doesn't need to collect identifiable data. Utah DPA V2 b: Vendor provided sufficient response and requested redaction.

014[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Metadata on user interaction		x	
Student email		x	x
Student name	x	x	x
Unique user identifier	x	x	
Student other indicator information		x	x
Student app assigned ID number	x		
Student assessment, other*	x		
Student scheduled courses	x		
Student scheduled courses	x		
Student course data	x		
Student course grades	x		
Student course grades/performance scores	x		
Student generated content	x		
Student in-app performance	x		
Student IP address	x		
Student local ID number	x		
Student online communications	x		
Student other**	x		
Student, other**	x		
Other**	x		
Student demographics, other**	x		
Student, other**	x		
Student school enrollment	x		
Student survey/questionnaire responses	x		
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	19
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
**Free-text data element description removed to maintain vendor confidentiality.

015[b] (student account)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username		x	
Student app password		x	
Student IP address		x	

Additional Details	
LEAs using this app	12
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: DPA indicates that no data is collected.
UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

015[b] (teacher account)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username		x	
Student app password		x	
Student IP address		x	

Additional Details	
LEAs using this app	12
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: DPA indicates that no data is collected.
UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

016[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student email	x	x	x
Student IP address	x	x	
Metadata on user interaction	x		
Student name	x	x	x
Student birthdate		x	
Other:**		x	
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	67
Number of 3rd parties receiving data	6
Number of advertising related entities receiving data	5*
Aggregator platforms receiving data	Google, Microsoft

Notes: Provided under statewide agreement. A DPA exists, as well: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.
**Free-text data element description removed to maintain vendor confidentiality.

017[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app assigned ID number	x		
Student app password	x	x	
Student app username	x	x	
Student grade level	x	x	
Student year of graduation	x		
Student IP address	x	x	
Metadata on user interaction	x		
Student name	x	x	x
Student teacher/counselor names	x		
Parent/Guardian email		x	
Unique user identifier	x	x	x
Student in-app performance		x	x

Additional Details	
LEAs using this app	47
Number of 3rd parties receiving data	4
Number of advertising related entities receiving data	2*
Aggregator platforms receiving data	Google, Microsoft

Notes: Vendor-Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

018[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username		x	
Student in-app performance		x	
Student IP address	x	x	x
Unique user identifier	x	x	x
Meta data on user interaction	x		
Student gender (Optional)	x		
Student language information (Optional)	x		
Student school enrollment	x		
Student grade level	x		
Parent email	x		
Student birthdate (Optional)	x		
Student teacher names	x		
Student language information (Optional)	x		
Student low income status	x		
Student specialized education services	x		
Student local school ID number	x		
Student app assigned ID number	x		
Student name	x		

Additional Details	
LEAs using this app	16
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google, Microsoft*

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that their educational offerings do not utilize Microsoft nor Google.

019[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app-assigned ID number	x		
Student app password	x	x	
Student app username	x	x	
Student birthdate	x	x	
Student scheduled courses	x		
Student generated content	x		
Student grade level	x		
Student in-app performance	x	x	x
Student IP address	x	x	
School local ID number	x		
Metadata on user interaction	x		
Student metadata, other*	x		
Student name	x	x	x
Student school enrollment	x		
Student questionnaire/survey responses	x		
Student teacher/counselor names	x		
Student email		x	x
Student metadata, other*		x	x
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	40
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Microsoft

Notes: Utah DPA V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

020[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student birthdate	x	x	
Student email	x	x	
Student generated content	x		
Student IP address	x	x	
Student name	x		
Student questionnaire/survey responses	x		
Student in-app performance		x	
Metadata on user interaction		x	
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	83
Number of 3rd parties receiving data	5
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: No active agreement. Entry based on expired UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

021[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student IP address	x	x	
Student name		x	
Unique user identifier	x	x	
Student email		x	
Student in-app performance	x	x	
Metadata on user interaction	x	x	
Student generated content	x		
Student, other*	x		
Student, other*	x		
Metadata, other*	x		
Student specialized education services*	x		

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

022[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent email		x	
Student ID number		x	
Student name	x	x	
Student grade level	x		
School local ID number	x		
Student school enrollment	x		

Additional Details	
LEAs using this app	24
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

023[b] (teacher account)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username	x	x	
Student app password	x	x	
Teacher email		x	
Student grade level	x	x	
Student in-app performance	x	x	
Student IP address		x	
Student name	x	x	
Student teacher/counselor names	x	x	
Student assessment, other*	x		
Student enrollment, other*	x		
Metadata on user interaction	x		

Additional Details	
LEAs using this app	14
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

023[b] (student account)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username	x	x	
Student app password	x	x	
Student grade level	x	x	
Student in-app performance	x	x	
Student IP address		x	
Student name	x	x	
Student teacher/counselor names	x	x	
Student assessment, other*	x		
Student enrollment, other*	x		
Metadata on user interaction	x		

Additional Details	
LEAs using this app	14
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

024[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Metadata on user interaction	x		
Student app username	x	x	
Student app password	x	x	
Student name	x	x	
Student in-app performance		x	
Student IP address		x	

Additional Details	
LEAs using this app	15
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

Vocabulary Spelling City[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent/guardian email		x	
Parent/guardian name		x	
Student app password	x	x	
Student app username	x	x	
Student IP address	x	x	
Student assessment standardized test scores	x		
Student generated content	x		
Student grade level (optional)	x		
Metadata on user interaction	x		
Student name (optional)	x		

Additional Details	
LEAs using this app	20
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: Utah DPA V2: https://sdpc.a4l.org/agreements/VKIDZ_HOLDINGS_UT_DPA_V2_3142019.pdf
d: Vendor name not redacted due to nonresponse. USBE was unable to confirm a contact; the report was sent to their legal email address, but response was never received.

026[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student email	x	x	
Student generated content		x	
Student IP address	x	x	
Student birthdate	x		
Student demographic, other**	x		
Student name	x	x	
Unique user identifier	x	x	x
Student year of graduation	x		
Student local ID number	x		
Student enrollment, other**	x		
Metadata on user interaction	x		
Student school enrollment	x		
Student specific curriculum programs	x		
Student survey/questionnaire responses	x		
Student grade level	x		

Additional Details		
LEAs using this app		6
Number of 3rd parties receiving data		54
Number of advertising related entities receiving data		54*
Aggregator platforms receiving data	Amazon, Google, Microsoft	

Notes: DPA is for education edition. Testing was performed on a standard account.
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.
**Free-text data element description removed to maintain vendor confidentiality.

027[b] (first test)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Unique user identifier		x	x

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	9
Number of advertising related entities receiving data	8
Aggregator platforms receiving data	Google

Notes:UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

027[b] (second test)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

028[b] (teacher account)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student enrollment, other**		x	
Unique user identifier	x	x	x
Student IP address	x		

Additional Details	
LEAs using this app	32
Number of 3rd parties receiving data	10
Number of advertising related entities receiving data	8*
Aggregator platforms receiving data	Google, Microsoft, Twitter

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor made configuration changes as requested to remove these.
**Free-text data element description removed to maintain vendor confidentiality.

028[b] (student account)

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student enrollment, other**		x	
Unique user identifier	x	x	x
Student IP address	x		

Additional Details	
LEAs using this app	32
Number of 3rd parties receiving data	10
Number of advertising related entities receiving data	8*
Aggregator platforms receiving data	Google, Microsoft, Twitter

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor made configuration changes as requested to remove these.
**Free-text data element description removed to maintain vendor confidentiality.

029[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent/guardian email		x	
Student app password	x	x	
Student IP addresses	x	x	
Unique user identifier	x	x	x
Student app username	x		
Student name	x		
Student in-app performance	x		
School local ID number	x		
Metadata on user interactions	x		
Student state ID number SSID	x		
Student app assigned ID number	x		
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	12
Number of 3rd parties receiving data	8
Number of advertising related entities receiving data	7*
Aggregator platforms receiving data	Facebook, Google, Microsoft

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

030[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Unique user identifier		x	x

Additional Details	
LEAs using this app	28
Number of 3rd parties receiving data	4
Number of advertising related entities receiving data	4*
Aggregator platforms receiving data	Google, Facebook

Notes: Vendor-Specific DPA
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that advertising in their paid service is not targeted or behavioral, thus adhering to FERPA, COPPA, and Utah state laws.

031[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	
Student email	x	x	
Student IP address	x	x	
Student name	x	x	
Unique user identifier	x	x	x
Student generated content	x		
Metadata on user interaction	x		
Metadata, other**	x		

Additional Details	
LEAs using this app	17
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	2*
Aggregator platforms receiving data	Amazon, Microsoft

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.
**Free-text data element description removed to maintain vendor confidentiality.

032[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student email		x	
Student grade level	x	x	
Student in-app performance	x	x	
Student IP address	x	x	
Student name	x	x	
Unique user identifier	x	x	x
Student app assigned ID number	x		
Student app password	x		
Student app username	x		
Student assessment, other**	x		
Metadata on user interactions	x		
Parent/guardian email	x		

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Google

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor removed the identified tracking pixel, which was inadvertently included on certain student-facing pages.
**Free-text data element description removed to maintain vendor confidentiality.

033[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student email	x	x	x
Student name	x	x	x
Unique user identifier		x	x
Student app assigned ID number	x		
Student app password	x		
Student app username	x		
Student grade level	x		
Student in-app performance	x		
Metadata on user interaction	x		
Student school enrollment	x	x	x
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	4
Number of 3rd parties receiving data	4
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Google

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that the identified traffic was anonymous but chose to remove it, as requested.

034[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student email	x	x	
Student generated content		x	
Student IP address	x	x	
Metadata on user interaction	x	x	
Student name	x	x	
Unique user identifier	x	x	x
Student language information	x		
Student online communications	x		

Additional Details	
LEAs using this app	9
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Microsoft, Google

Notes: Vendor Specific NDPA
b: Vendor provided sufficient response and requested redaction.

035[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student email	x	x	
Student in-app performance	x		
Student IP address	x	x	
Student name	x	x	x
Student app password		x	
Unique user identifier	x	x	

Additional Details	
LEAs using this app	38
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

036[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Unique user identifier	x	x	x
Student app password	x	x	
Student app username	x	x	
Student assessment results	x		
Student course data	x		
Student scheduled courses	x		
Student course grades/performance scores	x		
Student generated content	x		
Student grade level	x		
Student IP address	x		
Student local ID number	x		
Metadata on user interaction	x		
Student name	x		
Student language information	x		
Student online communications	x		
School enrollment	x		
Student teacher/counselor names	x		
Student app assigned ID number	x		
Student email		x	
Parent/Guardian email	x		

Additional Details	
LEAs using this app	15
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.

037[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password		x	
Student email	x	x	x
Student IP address	x	x	
Unique user identifier	x	x	x
Student metadata, other*	x		
Student name	x		x
Student other*	x		

Additional Details	
LEAs using this app	18
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Microsoft

Notes: Vendor Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

Wakelet[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student birthdate		x	
Student email	x	x	
Student IP address	x	x	
Metadata on user interaction	x	x	
Student name	x	x	
Student generated content	x		
Unique user identifier	x	x	x
Student grade level	x		
Other: profile image, profile bio, any items saved to Wakelet collections	x		
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: DPA expired in December 2024. Vendor Specific UT-NDPA-V1: https://sdpc.a4l.org/agreements/Wakelet%20Limited__UT_NDPA_V1_1.pdf
d: Vendor name not redacted due to nonresponse. USBE was able to confirm a contact, but they never responded once the letter was sent.

039[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username	x	x	
Student app password	x	x	
Student IP address	x	x	
Student teacher/counselor names		x	
Metadata on user interaction	x		
Student name	x		
Student survey results	x		

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

Destiny Discover[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student address	x		
Student app assigned ID number	x		
Student app password	x		
Student app username	x		
Student address (mailing)	x		
Student birthdate	x		
Student scheduled courses	x		
Student email	x		
Student ethnicity or race	x		
Student gender	x		
Student generated content	x		
Student grade level	x		
Student year of graduation	x		
Student homeroom	x		
Student IP address	x		
Student local ID number	x		
Metadata on user interactions	x		
Student name	x		
Student, other: library barcode	x		
Student other: patron type and status	x		
Student, other: card expiration date	x		
Student, other: student photo/image	x		
Student phone	x		
Student school enrollment	x		
Student teacher/counselor names	x		
Student enrollment, other: school location		x	
Parent/guardian address	x		
Parent/guardian email	x		
Parent/guardian phone number	x		
Parent/guardian first and/or last name	x		

Additional Details	
LEAs using this app	18
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: Vendor Specific UT-NDPA-V1: https://sdpc.a4l.org/agreements/Legacy Prep - Follett DPA v2.pdf
d: Vendor name not redacted due to nonresponse. USBE attempted to contact the email address on the DPA but received no response; reaching out to their support email afterward yielded no response, either.

041[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x		
Student app username	x		
Student assessment results	x		
Student class attendance data	x		
Student email	x	x	
Student generated content	x		
Student grade level	x		
Student in-app performance	x	x	
Student IP address	x		
Student local ID number	x		
Metadata on user interaction	x		
Student name	x	x	
Student teacher/counselor names	x		
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	54
Number of 3rd parties receiving data	33
Number of advertising related entities receiving data	33*
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

042[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student IP address	x	x	
Unique user identifier	x	x	x
Student email	x		
Student name	x		

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	11
Number of advertising related entities receiving data	9*
Aggregator platforms receiving data	Microsoft, Google

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

Study.com[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student email	x	x	
Student app password	x	x	
Student IP address	x	x	
Student name	x	x	
Unique user identifier	x	x	x
Student app assigned ID number	x		
Student app username	x		
Student course data	x		
Student course grades	x		
Student course grades/performance scores	x		
Student grade level	x		
Student in-app performance	x		
Metadata on user interaction	x		
Student survey/questionnaire responses	x		
Parent/guardian ID number	x		
Parent/guardian email address	x		

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	6
Number of advertising related entities receiving data	6
Aggregator platforms receiving data	Google, Microsoft, Twitter (X), Facebook

Notes: Utah DPA V2: https://sdpc.a4l.org/agreements/Study.com DPA w:Exhibit E_1
d: Vendor name not redacted due to nonresponse. USBE attempted to contact the email on the DPA but received no response, which was then followed by attempts to their privacy email address, which also yielded no response.

Conjuguemos[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app-assigned ID number	x		
Student app username	x	x	
Student IP address	x	x	
Student name	x	x	
Unique user identifier	x	x	x
Student email	x		
Student in-app performance	x		
Metadata on user interaction	x		

Additional Details	
LEAs using this app	9
Number of 3rd parties receiving data	5
Number of advertising related entities receiving data	4
Aggregator platforms receiving data	Amazon, Google

Notes: Utah DPA V2: https://sdpc.a4l.org/agreements/Conjuguemos DPA w:Exhibit E_2.pdf
d: Vendor name not redacted due to nonresponse. While the vendor did not submit a formal response, they expressed a desire to work with USBE. They were waiting to finalize the redesign of their website and were unable to submit a response in time.

045[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent/guardian email	x	x	
Student app password	x	x	
Student app username	x	x	x
Student IP address	x	x	
Student name	x	x	
Unique user identifier	x	x	x
Metadata on user interaction	x		
Student assessment data	x		
Student class attendance data	x		
Student school enrollment	x		
Student grade level	x		
Student homeroom	x		
Student curriculum programs	x		
Parent/guardian address	x		
Parent/guardian first and/or last name	x		
Student scheduled courses	x		
Student teacher names	x		
Student email	x		
Student local ID number	x		
Student app assigned ID number	x		
Student in-app performance	x		
Student generated content	x		
Student course grades	x		
Student course data	x		
Student course grades/performance scores	x		

Additional Details	
LEAs using this app	16
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	3
Aggregator platforms receiving data	Google, Microsoft

Notes: UT-NDPA-V1
b: Application was acquired between testing and publication; vendor did not respond to the original request but was offered redaction due to the positive privacy practices of their new ownership.

046[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student name	x	x	
Student grade level	x	x	
Student IP address	x	x	
Student teacher names	x		
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	3*
Aggregator platforms receiving data	Microsoft, Google

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service. Vendor also made requested changes on their educator-facing site.

047[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent/guardian email	x	x	
Parent/guardian ID number	x		
Student app password	x	x	
Student email	x		
Unique user identifier	x	x	x
Student app assigned ID number	x		
Student app username	x		
Student scheduled courses	x		
Student English language learner information	x		
Student gender	x		
Student generated content	x		
Student grade level	x		
Student homeroom	x		
Student in-app performance	x		
Student IP address	x		
Student ethnicity/race	x		
Student specific curriculum programs	x		
School local ID number	x		
Student state ID number (SSID)	x		
Metadata on user interaction	x		
Student name	x		
Student school enrollment	x		
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	26
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	3*
Aggregator platforms receiving data	Microsoft

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

048[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student in-app performance	x	x	
Student IP address	x	x	
Metadata on user interaction	x	x	
Student name	x	x	
Unique user identifier	x	x	x
Student app assigned ID number	x		
Student app username	x		
Student grade level	x		
Student school enrollment	x		
Student survey/questionnaire responses	x		
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	2*
Aggregator platforms receiving data	Microsoft, Google

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

049[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student IP address	x	x	
Unique user identifier	x	x	x
Metadata on user interaction	x		
Student online communications	x		
Student graduation year	x		
Student email	x		
Student phone	x		
Student app assigned ID number	x		
Student app password	x		
Student name	x		
Student extracurricular activities	x		
Student questionnaire/survey	x		

Additional Details	
LEAs using this app	11
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	2*
Aggregator platforms receiving data	Google, Twitter, Microsoft

Notes: Vendor Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

050[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x		
Student app username	x		
Student standardized test scores	x		
Student class attendance data	x		
Student email	x	x	
Student in-app performance	x	x	
Student IP address	x		
Student local ID number	x		
Metadata on user interaction	x		
Student name	x	x	
Student assessment observation data	x		
Student online communications	x		
Student survey/questionnaire responses	x		
Student teacher/counselor names	x		
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	29
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	2*
Aggregator platforms receiving data	Google

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

051[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username	x	x	
Student app password	x	x	
Student email (optional)	x	x	x
Student generated content	x	x	
Student IP address	x	x	
Student name (optional)	x	x	x
Unique user identifier	x	x	x
Student app assigned ID number	x		
Student standardized test scores (optional)	x		
Student English language learner information (optional)	x		
Student ethnicity or race (optional)	x		
Student grade level	x		
Student in-app performance	x		
Student low income status (optional)	x		
School local ID number (optional)	x		
Metadata on user interactions	x		
Metadata, other*	x		
Student observation data	x		
Student school enrollment	x		
Student specialized education services*	x		
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	15
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	2
Aggregator platforms receiving data	Google, Microsoft

Notes: Utah DPA V2
*Free-text data element description removed to maintain vendor confidentiality.

052[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Parent email	x	x	
Student birthdate	x	x	
Student email	x	x	
Student ethnicity/race	x	x	
Student gender	x	x	
Student grade level	x	x	
Student name	x	x	
Student phone	x	x	
Student school enrollment	x	x	
Unique user identifier	x	x	x
School local ID number	x		
Student address	x		
Student app assigned ID number	x		
Student app username	x		
Student app password	x		
Student extracurricular activities	x		
Student grade level	x		
Student year of graduation	x		
Student IP address	x		
Metadata on user interaction	x		
Student metadata, other**	x		
Student demographics, other**	x	x	
Student, other**	x		
Student, other**	x		
Student, other**	x		
Student, other**	x		
Student questionnaire/survey responses	x		

Additional Details	
LEAs using this app	25
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Google

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.
**Free-text data element description removed to maintain vendor confidentiality.

053[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student IP address	x	x	
Student email	x	x	
Student local ID number	x		
Student name	x	x	
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Google

Notes: Out-of-state DPA
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

054[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app assigned ID number	x		
Student app password	x	x	
Student app username	x	x	x
Student assessment, other**	x		
Student email (optional)	x	x	x
Student gender	x		
Student generated content	x		
Student course grades/performance scores	x		
Student in-app performance	x	x	
Student IP address	x	x	
Metadata on user interaction	x		
Student name	x	x	x
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	32
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Microsoft

Notes: Vendor Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.
**Free-text data element description removed to maintain vendor confidentiality.

055[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username	x	x	
Student app password	x	x	
Student IP address	x		
Metadata on user interaction	x		
Student in-app performance	x		
Unique user identifier	x	x	x
Parent/guardian email	x		

Additional Details	
LEAs using this app	23
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Twitter

Notes: Vendor Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor removed the requested, unintentional social media integration.

056[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username	x	x	
Student app password	x	x	
Student email	x	x	
Student generated content	x	x	
Student IP address	x	x	
Unique user identifier	x	x	x
Student app assigned ID number	x		
Metadata on user interaction	x		
Student name	x		
Student online communications	x		
Student survey/questionnaire responses	x		
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	9
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Google

Notes: Vendor Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Vendor modified a video embedding configuration to address the requested action.

GMetrix[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student IP address	x	x	
Unique user identifier	x	x	x
Student assessment, other: practice test proficiency and completion	x		
Student email	x		
Metadata on user interaction	x		
Student name	x		
Student language information	x		
Student other indicator information, other: ADA accommodation usage	x		

Additional Details	
LEAs using this app	19
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	1
Aggregator platforms receiving data	Google

Notes: All listings were indicated "inactive." Utah DPA V2: https://sdpc.a4l.org/agreements/Gmetrix 2.0.pdf
d: Vendor name not redacted due to nonresponse. The individual working with the USBE representative left the company; response was not provided.

Read Theory[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student IP address	x	x	
Unique user identifier	x	x	x
Metadata on user interaction	x		
Student school enrollment	x		
Student grade level	x		
Student homeroom	x		
Student email	x		
Student app-assigned ID number	x		
Student name	x		
Student in-app performance	x		

Additional Details	
LEAs using this app	19
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/2023-10-05_6582_11030_signed_agreement_file.pdf
d: Vendor name not redacted due to nonresponse. The USBE representative sent the letter to one of their support agents after being unable to contact the vendor from the email address on the DPA; USBE did not receive a follow-up response.

059[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Unique user identifier	x	x	x
Student assessment, other*	x		
Student grade level (optional)	x		
Student IP address	x		
Metadata on user interaction	x		
Student name (optional)	x		
Student teacher/counselor names	x		
Parent/guardian email	x		
Parent/guardian phone	x		
Parent/guardian first and/or last name	x		

Additional Details	
LEAs using this app	39
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Microsoft

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

060[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app assigned ID number	x		
Student app password	x	x	
Student app username	x	x	
Student email	x	x	
Student generated content	x		
Student grade level	x	x	
Student IP address	x	x	
Metadata on user interaction	x		
Student name	x		
Parent/guardian email	x	x	

Additional Details	
LEAs using this app	43
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

061[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student email	x		
Student generated content	x		
Student generated content, other*	x		
Student IP address	x		
Metadata on user interaction	x		
Student name	x		
Student online communications	x		
Student school enrollment	x		
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	26
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: Vendor Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

062[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student grade level	x	x	
Student in-app performance	x	x	
Student IP address	x	x	
Meta data on user interaction	x	x	x
Student name	x	x	
Student other*	x		
Unique user identifier	x	x	x
Student app assigned ID number	x		
Student state ID number SSID	x		
Parent ID number	x		
Other metadata*	x		
Other metadata*	x		

Additional Details	
LEAs using this app	15
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Microsoft

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

063[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username	x	x	
Student app password (Optional)	x	x	
Student in-app performance	x	x	
Student IP address	x	x	
Metadata on user interactions	x	x	
Other Application Meta Data	x		
Standardized test scores (optional)	x		
Other Assessment Data (Optional)	x		
Language information	x		
Student school enrollment	x		
Student grade level	x		
Teacher names	x		
Teacher emails	x		
Local (School district) ID number (Optional)	x		
Student responses to surveys or questionnaires	x		
Student generated content	x		
Student name	x	x	

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

Happy Numbers (Student)[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student standardized test scores	x	x	
Student grade level	x	x	
Student in-app performance	x	x	
Student IP address	x	x	
Metadata on user interaction	x	x	
Student name	x	x	
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	12
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Amazon, Facebook, Google

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/2024-05-01_6583_1018_signed_agreement_file.pdf
d: Vendor name not redacted due to nonresponse. The USBE representative confirmed a contact but never received a subsequent response after providing the letter.

Happy Numbers (Teacher)[d]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x		
Student app username	x	x	
Student standardized test scores	x	x	
Student grade level	x	x	
Student in-app performance	x	x	
Student IP address	x		
Metadata on user interaction	x		
Student name	x	x	
Student teacher/counselor names	x		

Additional Details	
LEAs using this app	12
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Amazon, Facebook, Google

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/Happy Numbers DPA w:Exhibit E.pdf
d: Vendor name not redacted due to nonresponse. The USBE representative confirmed a contact but never received a subsequent response after providing the letter.

065[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student email	x	x	
Student generated content	x	x	
Metadata on user interaction	x	x	
Student name	x	x	
Student app assigned ID number	x		
Student app username	x		
Parent/guardian email	x		

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: Utah DPA V2
b: Vendor provided sufficient response and requested redaction.

066[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student email	x	x	
Student app password	x	x	
Student IP address	x	x	
Student name	x	x	
Unique user identifier	x	x	x
Student app username	x		
Student generated content	x		
Student in-app performance	x		
Metadata on user interaction	x		
Student online communications	x		
Student survey/questionnaire responses	x		

Additional Details	
LEAs using this app	63
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: App is available under statewide agreement and UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

067[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student name	x	x	
Student IP address	x	x	
Student grade level	x	x	
Student app assigned ID number	x		
Student app password	x		
Student app username	x		
Student assessment results	x		
Student in-app performance	x		
Metadata on user interaction	x		
Student school enrollment	x		
Student teacher/counselor names	x		
Parent/Guardian email	x		
Parent/Guardian ID number	x		
Parent/Guardian first and/or last name	x		
Student English language learner information	x		
Student Local ID number	x		

Additional Details	
LEAs using this app	12
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.

068[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app assigned ID number	x		
Student app password	x		
Student app username	x		
Student assessment results (optional)	x		
Student birthdate (optional)	x		
Student scheduled courses	x		
Student email (optional)	x		
Student English language learner information (optional)	x		
Student ethnicity or race (optional)	x		
Student gender (optional)	x		
Student grade level	x		
Student homeroom (optional)	x		
Student IP addresses	x	x	
School local ID number	x		
Metadata on user interactions	x		
Student name	x		
Student language information	x		
Student, other*	x		
Student school enrollment	x		
Student specific curriculum programs	x		
Student state ID number SSID (optional)	x		
Student teacher/counselor names	x		
Parent/guardian email (optional)	x		
Parent/guardian ID (optional)	x		
Parent/guardian name (optional)	x		

Additional Details	
LEAs using this app	13
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: Vendor Specific UT-NDPA-V1
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

Arduino[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app username	x	x	
Student app password	x	x	
Student email	x	x	
Student IP address	x	x	
Meta data on user interaction	x		
Student teacher/counselor names	x		
Parent/Guardian Email	x		
Parent/Guardian ID	x		

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/Arduino SRL NDPAv1 signed.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

Boom Cards[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app assigned ID number	x		
Student app password	x	x	
Student app username	x	x	
Student assessment, other: formative and summative as assigned by the teacher	x		
Student conduct behavior discipline incident information (only to the extent to which an educator creates or assigns a Boom Cards resource that collects such information)	x		
Student email (– Where the Educator uses an authentication method that supplies an email)	x	x	
Student generated content (short written answers; eventually, student created decks)	x		
Student work data, other: fill in the blank, multiple choice, and other responsive choices			
Student grade level (can be inferred if educator provides the information)	x		
Student in-app performance (– yes if the Educator assigns using student performance collection; Educators may avoid by using only Fastplay assignments.)	x		
Use of cookies, etc.	x	x	
School local ID number (where included in student email address (we do not extract it))	x		
Metadata on user interaction (last login)	x		
Metadata, other: platform, browser, build number	x		
Student name (yes as most Educators provide actual names; pseudonyms are allowed)	x	x	
Online communications (educator to publishing public author feedback)	x		
Student demographics, other: school location can be inferred from teacher's or student's email domain of school account	x		
Student specific curriculum programs (possible to infer from educator assigned content)	x		
Student survey/questionnaire responses (when an Educator assigns a Boom Cards mini-app that functions as a survey or questionnaire)	x		
Student teacher/counselor names (when provided by the educator)	x		

Additional Details	
LEAs using this app	38
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: Vendor Specific UT-NDPA-V1: https://sdpc.a4l.org/agreements/2023-07-07_6570_6582_signed_agreement_file.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

Code Combat (student)[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student email	x	x	x
Student in-app performance	x	x	
Student IP address	x	x	
Metadata on user interaction	x	x	
Unique user identifier	x	x	x
Student generated content	x		
Student name	x		
Student language information	x		

Additional Details	
LEAs using this app	12
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Facebook, Google, Twitter*

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/UT_NDPA_V1_CODECOMBAT.pdf
a: Vendor provided sufficient response regarding analytics/aggregator platforms and opted to remain named in the published report.
*Vendor indicated that all social media integrations are disabled for student accounts.

Code Combat (teacher)[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x		
Student app username	x		
Student email	x	x	x
Student in-app performance	x	x	
Student IP address	x	x	
Meta data on user interaction	x		
Unique user identifier	x	x	x
Student generated content	x		
Student name	x		
Student language information	x		

Additional Details	
LEAs using this app	12
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Facebook, Google, Twitter*

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/UT_NDPA_V1_CODECOMBAT.pdf
a: Vendor provided sufficient response regarding analytics/aggregator platforms and opted to remain named in the published report.
*Vendor indicated that all social media integrations are disabled for student accounts.

Code.org[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app assigned ID number	x		
Student app password	x	x	
Student app username	x	x	
Student assessment results, other: student answers to assessments in Code.org coursework	x		
Student birthdate (age, not date of birth)	x	x	
Student email	x		
Student ethnicity or race	x		
Student gender	x	x	
Student generated content	x		
Student grade level	x		
Student in-app performance	x		
Metadata on user interaction	x		
Student name	x		
Student school enrollment	x		
Student responses to surveys/questionnaires	x		
Student teacher/counselor names	x		
Student IP address	x	x	
Parent/guardian email	x		
Metadata, other: log files	x		
Metadata, other: cookies	x		
Metadata, other: web beacons/pixel tags	x		

Additional Details	
LEAs using this app	65
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: Vendor Specific UT-NDPA-V1: https://sdpc.a4l.org/agreements/2023-12-07_6988_234_signed_agreement_file.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

CodeHS[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app assigned ID number	x		
Student app password	x		
Student app username	x		
Student class attendance data	x		
Student course data	x		
Student course grades	x		
Student course grades/performance scores	x		
Student email	x	x	
Student generated content	x	x	
Student in-app performance	x	x	
Student IP address	x		
Student name	x	x	
Student survey results	x		
Student teacher/counselor names	x		
Unique user identifier	x	x	x

Additional Details	
LEAs using this app	31
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/2023-08-31_6590_873_signed_agreement_file.pdf
a: Vendor provided sufficient assurances regarding the anonymity of their analytics and chose to remain named in the published report.

Desmos[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app assigned ID number	x		
Student app password	x	x	
Student app username	x		
Student school (daily) attendance information	x		
Student class attendance data	x		
Student scheduled courses	x		
Student email	x	x	
Student generated content	x		
Student grade level	x		
Student in-app performance	x		
Student IP address	x		
School local ID number	x		
Metadata on user interactions	x		
Student name	x	x	
Student language information	x		
Student assessment observation data	x		
Student school enrollment	x		
Student specific curriculum programs	x		
Student survey/questionnaire responses	x		
Student teacher/counselor names	x		
Parent/guardian phone number	x		
Parent/guardian ID	x		
Parent/guardian email	x		
Parent/guardian first and/or last name	x		
Metadata, other: device type, browser model, screen resolution	x		
Demographic, other: incidental data from free text responses from students	x		
Demographic, other: student-selected accessibility preferences	x		

Additional Details	
LEAs using this app	43
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: Vendor specific UT-NDPA-V1: https://sdpc.a4l.org/agreements/UT-%20Promontory%20School%20Desmos%20NDPA_V1_executed_2021_5_3.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

Educreations[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student email	x	x	
Student IP addresses	x	x	
Student name	x	x	
Student generated content	x		
Metadata on user interactions	x		
Student online communications	x		

Additional Details	
LEAs using this app	10
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: Utah DPA V2: https://sdpc.a4l.org/agreements/Educreations DPA w:Exhibit E_1.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

Kami App[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student email	x	x	
Student generated content	x		
Student IP address	x	x	
Metadata on user interaction	x		
Student assessment observation data	x		
Student app-assigned user ID	x		
Student name	x	x	
Student course data	x		
Student course grades/performance scores	x		
Unique user identifier	x	x	

Additional Details	
LEAs using this app	27
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/2024-03-21_6583_260_signed_agreement_file.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

Starfall[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student IP address	x	x	
Other application technology metadata	x		

Additional Details	
LEAs using this app	34
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: UT-NDPA-V1: https://sdpc.a4l.org/agreements/2022-09-28_6597_392_signed_agreement_file.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

Typing Club[a]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student app password	x	x	
Student app username	x	x	
Student email	x	x	
Student IP address	x	x	
Student name	x	x	
Student app assigned ID number	x		
Student assessment, other: typing test	x		
Student grade level	x		
Student in-app performance	x		
Student local ID number	x		
Metadata on user interaction, other: browser type/user agent	x		
Student school enrollment	x		
Student course grades/performance scores	x		

Additional Details	
LEAs using this app	23
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: DPA is for the education edition. UT-NDPA-V1s: https://sdpc.a4l.org/agreements/UT_NDPA_V1_TypingClub_Cache_1_1.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

Tinkercad[a]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student app username		x	
Student app password		x	
Student birthdate		x	
Student IP address		x	
Additional Details			
LEAs using this app			29
Number of 3rd parties receiving data			0
Number of advertising related entities receiving data			0
Aggregator platforms receiving data			

Notes: Tinkercad uses a custom DPA that is not from the SDPC website: https://sdpc.a4l.org/agreements/2022-10-03_6597_58_signed_agreement_file.pdf
a: The review did not indicate any identified issues or requested actions; the vendor opted to remain named in the published report.

080[b]

Data Elements	Agreement allowed	Tested actual	Shared with 3rd parties
Student assessment results		x	
Student assignment scores		x	
Student birthdate		x	
Student email		x	
Student grade level		x	
Student in-app performance		x	
Student IP address		x	x
Student name		x	
School enrollment		x	
Unique user identifier		x	x

Additional Details	
LEAs using this app	67
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: Custom DPA
b: Vendor provided sufficient response and requested redaction.

081[b]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student app password		x	
Student app username		x	
Student email		x	
Student IP address		x	
Metadata on user interaction		x	
Student name		x	
Unique user identifier		x	

Additional Details	
LEAs using this app	56
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Microsoft

Notes: Privacy Policy/Custom DPA
b: Vendor provided sufficient response and requested redaction.

082[b]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student enrollment, other*		x	
Student name		x	
Student birthdate		x	
Student email		x	
Unique user identifier		x	

Additional Details	
LEAs using this app	86
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: Privacy Policy/Custom DPA
b: Vendor provided sufficient response and requested redaction.
*Free-text data element description removed to maintain vendor confidentiality.

Spotify[d]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student app password		x	
Student app username		x	
Student birthdate		x	
Student email		x	
Student gender		x	
Unique user identifier		x	x

Additional Details	
LEAs using this app	9
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	2
Aggregator platforms receiving data	Google, Twitter(X)

Notes: No DPA. Their privacy policy can be found at: https://www.spotify.com/us/legal/privacy-policy/. It states openly that personal data will be used for marketing and advertising purposes.
d: Vendor name not redacted due to nonresponse. The USBE representative reached out to their privacy email but received no response.

084[b]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student app password		x	
Student birthdate		x	
Student email		x	
Student IP address		x	
Meta data on user interaction		x	
Unique user identifier		x	x

Additional Details	
LEAs using this app	47
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	2
Aggregator platforms receiving data	Google, Twitter(X)

Notes: Privacy Policy/iKeepSafe
Vendor's privacy policy states that they may use personal data for advertising. Reportedly, schools and districts are not providing student data to this application.
b: Vendor provided sufficient response and requested redaction.

085[b]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student IP address		x	x
Student user interaction data		x	x
Student city		x	
Student state		x	
Student zip code		x	x
Unique user identifier		x	x

Additional Details	
LEAs using this app	18
Number of 3rd parties receiving data	3
Number of advertising related entities receiving data	1*
Aggregator platforms receiving data	Google

Notes: Privacy Policy
b: Vendor provided sufficient response and requested redaction.
*Vendor provided assurances that this advertising is justifiable and not targeted/adheres to their privacy policy, FEPRA, and COPPA.

086[b]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Parents email		x	
Student app password		x	
Student app username		x	x
Student in-app performance		x	
Student birthdate		x	

Additional Details	
LEAs using this app	38
Number of 3rd parties receiving data	2
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google, Facebook

Notes: No DPA; privacy policy only.
b: Vendor provided sufficient response and requested redaction.

Scratch[d]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Unique user identifier		x	x
Student app password		x	
Student app username		x	
Student birthdate		x	
Student email		x	
Student gender		x	
Student generated content		x	
Student images		x	
Student IP address		x	
Meta data on user interaction		x	
Student country		x	
Additional Details			
LEAs using this app			28
Number of 3rd parties receiving data			1
Number of advertising related entities receiving data			0
Aggregator platforms receiving data			Google

Notes: There is no DPA or other contract for Scratch. Their privacy policy is available at: https://scratch.mit.edu/privacy_policy and it claims they will not share data with third party advertisers.
d: Vendor name not redacted due to nonresponse. The USBE representative attempted to contact the email address from their privacy policy but did not receive a response.

088[b]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student app password		x	
Student app username		x	
Student assignment scores		x	
Student email		x	x
Student in-app performance		x	
Student IP address		x	
Student name		x	x
School enrollment		x	x
Student teacher/counselor names		x	
Unique user identifier		x	x
School location		x	x

Additional Details	
LEAs using this app	92
Number of 3rd parties receiving data	5
Number of advertising related entities receiving data	2*
Aggregator platforms receiving data	Google, Microsoft

Notes: Statewide agreement
b: Vendor provided sufficient response and requested redaction.
*Vendor indicated that targeted advertising/tracking pixels are not present on student-facing site and/or paid education-specific service.

Utah Aspire+

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Program uses a proprietary browser with built-in encryption. Any attempt to read and/or capture the data would cross the line into penetration testing and not possible without legal contracts with the issuing company.			

Additional Details	
LEAs using this app	95
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: No DPA. Falls under USBE contract

Utah RISE

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Program uses a proprietary browser with built-in encryption. Any attempt to read and/or capture the data would cross the line into penetration testing and not be possible without legal contracts with the issuing company.			

Additional Details	
LEAs using this app	75
Number of 3rd parties receiving data	0
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	

Notes: There is no DPA for this app

091[b]

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student app password		x	
Student app username		x	
Student email		x	
Student grade level		x	
Student IP address		x	
Student name		x	
Unique user identifier		x	x

Additional Details	
LEAs using this app	52
Number of 3rd parties receiving data	1
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google

Notes: Statewide agreement
b: Vendor provided sufficient response and requested redaction.

092[b] (student account)

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
App assigned ID		x	
Student app password		x	
Student app username		x	
Student assessment results		x	
Student assignment scores		x	
Student course data		x	
Student course grades		x	
Student email		x	
Student generated content		x	
Student grade level		x	
Student in-app performance		x	
Student IP address		x	
Student name		x	
Observed student data		x	
Unique user identifier		x	x

Additional Details	
LEAs using this app	114
Number of 3rd parties receiving data	4
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google, Microsoft*

Notes: Statewide agreement
b: Vendor provided sufficient response and requested redaction.
*Vendor disabled all analytics for student accounts.

092[b] (teacher account)

Data Elements	N/A, no agreement	Tested actual	Shared with 3rd parties
Student app assigned ID number		x	
Student app username		x	
Student assessment results		x	
Student assignment scores		x	
Student birthdates		x	
Student course data		x	
Student course grades		x	
Student grade level		x	
Student in-app performance		x	
Student name		x	
Student observation data		x	
Names of student's teachers/counselors		x	
Teacher name		x	
Teacher email		x	
Unique user identifier		x	x
Teacher time zone		x	
Teacher zip code		x	

Additional Details	
LEAs using this app	114
Number of 3rd parties receiving data	4
Number of advertising related entities receiving data	0
Aggregator platforms receiving data	Google, Microsoft

Notes: Statewide agreement
b: Vendor provided sufficient response and requested redaction.