Matthew J. Langley
(Bar No. 342846)
matt@almeidalawgroup.com
ALMEIDA LAW GROUP
849 W. Webster Avenue
Chicago, IL 60614
Tel.: (773) 554-9354
David J. George*
DGeorge@4-Justice.com
GEORGE, FELDMAN, MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Tel.: (561) 232-6002

Lori G. Feldman*
LFeldman@4-justice.com
Michael Liskow*
MLiskow@4-Justice.com
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel.: (718) 878-6433

Julie U. Liddell*
julie.liddell@edtech.law
Andrew Liddell*
andrew.liddell@edtech.law
EDTECH LAW CENTER PLLC
P.O. Box 300488
Austin, Texas 78705
Tel: (737) 351-5855

Counsel for Plaintiffs and the Proposed Class

* *pro hac vice* forthcoming

SUPERIOR COURT FOR THE STATE OF CALIFORNIA

COUNTY OF ORANGE

NICOLE REISBERG, on behalf of herself and her minor children M.C. 1 and M.C. 2, *individually and on behalf of all others similarly situated*,

Plaintiffs,

v.

SEESAW LEARNING, INC.,

Defendant.

Civ. No.

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA") CAL. PENAL CODE §§ 631, 632;

2. VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE §§ 502, *ET SEQ.*

3. VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL") CAL. BUS. & PROF. CODE § 17200, *ET SEQ.*

4. INVASION OF PRIVACY—

CALIFORNIA CONSTITUTION

5. INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS

6. INTRUSION UPON SECLUSION

7. UNJUST ENRICHMENT

JURY TRIAL DEMANDED

"Above all things I hope the education of the common people will be attended to, convinced that on their good sense we may rely with the most security for the preservation of a due degree of liberty."

- Thomas Jefferson to James Madison, 1787

"Education is the world's most data-mineable industry by far."

- Jose Ferreira, EdTech CEO, May 2014

"[Education technology] companies' mission isn't a social mission. They're there to create return."

- Michael Moe, EdTech investor, May 2014

INTRODUCTION

1. Nicole Reisberg, on behalf of, and as parent and guardian of, her minor children, M.C. 1 and M.C. 2 ("Plaintiffs"), as well as on behalf of all other similarly situated individuals, by and through their attorneys, brings this class action complaint for injunctive and monetary relief against Defendant Seesaw Learning, Inc. ("Seesaw") and make the following allegations based upon her and her children's knowledge, and upon information and belief as to all other matters.

2. Seesaw has monetized the personal and private information of millions of school-aged children without effective consent.

3. Seesaw's leading product is a K-6[1] education technology platform (the "Seesaw Platform"), which it markets as creating digital student portfolios that purport to track a student's learning progress. These portfolios extract and retain wide-ranging student data, such as photo images, videos, audio recordings, and student-created content. Seesaw provides that data to its customers, among which are schools and school districts, but also dozens of private companies.

[1] "K-6" refers to Kindergarten through sixth grade.

4. Seesaw's generation, collection, and use of such personal and private information exposes students to serious and irreversible risks to their privacy, property, and autonomy and harms them in ways that are both concealed and profound.

5. Neither students nor their parents[2] have agreed to this arrangement. To be effective, an agreement must be supported by informed, voluntary consent, by a person with authority to do so, in exchange for sufficient consideration.

6. None of those elements are met here.

7. First, any purported agreement is not informed: Seesaw does not adequately disclose to students, parents, or schools what information it collects and what it does with that information in a reasonably understandable manner. Instead, Seesaw materially misrepresents its data practices, for example, by falsely touting its commitment to student privacy, stating that it can be used in a manner compliant with Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, and representing that it complies with the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501, *et seq*.

8. Second, any purported agreement is not voluntary: because children are required to attend to school, they are coerced into submitting to Seesaw's data practices.

9. Third, any purported agreement lacks sufficient consideration: because children are already entitled to an education—which includes the right to use educational products and services provided by the school—Seesaw provides them with no additional benefit that would support any purported agreement.

10. Finally, any purported consent was not provided by a person with authority to do so. Seesaw's users are minors. As such, Seesaw must obtain their parents' consent before taking and using their personal and private information. However, Seesaw does not seek parental consent. Instead, Seesaw relies on the consent of school personnel alone. School personnel, however, do not have authority to provide such consent in lieu of parents. Thus, even if school personnel purport to have given consent on behalf of children, any such consent is ineffective.

[2] The term "parent" as used herein refers broadly to a child's parent or legal guardian.

11. Schools have always collected certain personal information belonging to students in order to provide education services, and they must be able to continue to do so—within the bounds of the law.[3] Until recently, that collection was limited and transparent: parents generally knew what information was collected, by whom, and for what purpose. But times—and technology—have changed.

12. Schools no longer do the collecting; corporate third parties do. The information taken is not only traditional education records, but thousands of data points that span a child's life. That information is not used exclusively for educational purposes; it is instead used by myriad unknown entities for commercial purposes. And companies' data-extractive business models do not prioritize positive student outcomes; they prizes "measurability," "scalability," and other corporate imperatives that are often unaligned with, and are even adversarial to, children's privacy and healthy development. Companies may not deny parents the ability to guide their children's lives by marketing to schools and concealing their practices behind opaque technology and false promises of improving education.

13. Privacy is a fundamental right. Seesaw may not require that children entirely forgo that right to receive the education to which they are legally entitled. And parents, by sending their children to school as is their right and duty, do not surrender their authority to decide what personal information may be collected about their children, who may access it, and how it may be used. Seesaw must be held to account for operating as though the fundamental rights of children and their parents do not exist.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to the California Constitution, Article VI § 10 and California Code of Civil Procedure § 410.10, because Defendant transacted business and committed the acts alleged herein in Orange County, California.

15. This Court has personal jurisdiction over Defendant because it is headquartered in and has its principal place of business in Orange County, California.

[3] In this lawsuit, Plaintiffs do not seek to prevent schools from collecting and using legally permissible information about their students in a legally permissible manner, such as contemplated under FERPA.

16. Venue is proper in this Court under Code of Civil Procedure sections 395 and 395.5 because a substantial part of the acts or omissions giving rise to this action occurred in this County.

THE PARTIES

17. M.C. 1 is a minor. At all relevant times, she has been a citizen of the state of California. M.C. 1 attended a public school in an Orange County, California school district. As part of her public schooling, she was required to access and use the Seesaw Platform, which she has accessed and used from her school-issued device.

18. M.C. 2 is a minor. At all relevant times, he has been a citizen of the state of California. M.C. 2 attended a public school in an Orange County, California school district. As part of his public schooling, he was required to access and use the Seesaw Platform, which he has accessed and used from his school-issued device.

19. Plaintiff Nicole Reisberg is the mother and legal guardian of M.C. 1 and M.C. 2. At all relevant times, she has been a citizen of the state of California.

20. Defendant Seesaw Learning is a corporation organized under the laws of the State of Delaware. It maintains a principal place of business at 548 Market Street, PMB 22502, San Francisco, California 94104.

FACTUAL ALLEGATIONS

I. Today's digital products and services make money by monetizing user data.

A. The modern internet is built on the surveillance-capitalist business model.

21. For two decades, vast numbers of consumer-facing technology companies have built their businesses according to a model that Harvard Business School professor emerita Shoshana Zuboff, among others, has described as "surveillance capitalism."[4] At the heart of that model is an "extraction imperative" that prioritizes maximal collection and monetization of user data.

22. Under surveillance capitalism, a technology provider is incentivized to:

a. generate and collect as much data as possible about a user through the user's

[4] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).

interaction with the technology provider's platform;

b. use the data the technology provider generates and collects about the user to make predictions about that user's future behavior, which the technology provider uses to build its own products and services and shares with third parties seeking to profit from that user;

c. surreptitiously and subconsciously influence the user's behavior using what it knows about the user—both to keep the user on the platform longer (increasing the volume of information available to collect) and to coerce the user to act as the technology provider has predicted (increasing the value of the provider's predictions); and

d. enable third parties to make significant decisions about the user that can affect her life and future.

23. Submission to this arrangement has become the cost of being online: in order to use the internet, an individual must "consent" to having these intimate dossiers built about them, which are used by countless entities to identify and target them, make predictions about them, manipulate their behavior, and influence decision-making about them.

24. Given the extractive and exploitative nature of the surveillance business model, its viability depends on keeping the public in the dark. Companies thus employ numerous tactics to keep users unaware of their data practices, such as opaque terms of service, contracts of adhesion, hidden data-generation and data-collection technologies, and coercive design techniques.

25. The practices of surveillance capitalism have become commonplace—not just in technology domains like search, ecommerce, and social media—but also in more traditional domains, such as healthcare, employment, lending, and insurance. Courts have routinely found undisclosed corporate practices in these domains to be unlawful. And if the surveillance business model is unfair when used against adults in ostensibly voluntary consumer contexts, it is unconscionable when used against school-aged children in the compulsory setting of education.

B. Education is "the world's most data-mineable industry by far."

26. The surveillance business model also underpins digital platforms used in elementary, middle, and high schools across the United States.

27. Simply by attending school as is their legal right and obligation, children are subjected

to the same intrusive and exploitative data practices as adults in non-compulsory settings: reams of their personal and private information are harvested to build intimately detailed profiles about them, which are then used by the collecting company, schools, and a host of other third parties to identify, target, manipulate, and influence decision-making about them.

28. By collecting and monetizing children's information, education technology or "EdTech,"[5] has become a $250 billion global industry that is projected to nearly triple by 2027.[6]

29. Investors have taken note. Investments in EdTech have surged from $500 million in 2010 to $16.1 billion in 2021.[7]

30. Rather than describing a defining feature of any digital service or product, "EdTech" describes the market that these companies target, namely, schools and school districts. In that sense, any technology company that markets to schools can be considered an EdTech company.

31. Education has been described by a leading executive as "the world's most data-mineable industry by far."[8]

32. As one leading EdTech investor explained, these investments are not philanthropic: the purpose of these private EdTech ventures "isn't a social mission . . . . They're there to create

[5] Although the term "educational technology" can be defined broadly to include purely theoretical or pedagogical practices, this Complaint uses "EdTech" to refer generally to "all the privately owned companies currently involved in the financing, production and distribution of commercial hardware, software, cultural goods, services and platforms for the educational market with the goal of turning a profit." Tanner Mirrlees and Shahid Alvi, *EdTech Inc.: Selling, Automating and Globalizing Higher Education in the Digital Age* (2019).

[6] Louise Hooper, et al., *Problems with Data Governance in UK Schools*, Digital Futures Commission, 5Rights Foundation (2022), available at https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf (last accessed May 1. 2025).

[7] Alex Yelenevych, *The Future of EdTech*, Forbes, Dec. 26, 2022, available at https://www.forbes.com/sites/forbesbusinesscouncil/2022/12/26/the-future-of-edtech/?sh=7c2924676c2f (last accessed May 1. 2025).

[8] Stephanie Simon, *The big biz of spying on little kids*, Politico, May 15, 2014, available at https://www.politico.com/story/2014/05/data-mining-your-children-106676 (last accessed May 1. 2025).

return."[9]

33. The result is that EdTech has overtaken K-12 education. School districts access an average of nearly 3,000 EdTech tools during a schoolyear.[10] A single student accesses nearly fifty EdTech tools per year.[11] It is thus impossible to overstate the influence and effect this industry has had on education and school-aged children.

II. Seesaw profits enormously from the personal information of millions of elementary-school children.

34. Seesaw contracts with schools and school districts to provide a host of services ranging from course management; assignment delivery and grading; communication between teachers, students, and parents; student-content delivery and management; and student-data analytics.

35. Public schools and school districts pay for Seesaw's services with government funds.

36. Seesaw does not provide products that merely serve as a kind of digital filing cabinet in which PK-6 schools may store education records.

37. Rather, Seesaw is an EdTech company specializing in data generation, collection, storage, and analytics.

38. As a result, since its launch in 2015, Seesaw has secured a total of $175 million in funding. As of January 2025, Seesaw's annual revenue was estimated to be $75 million dollars.

A. Seesaw has amassed vast troves of student data through its K-6-marketed products and data-sharing agreements.

39. Seesaw generates, collects, and otherwise obtains personal information belonging to, from, and about millions of school-aged children in the United States.

40. Seesaw's primary customers are schools and school districts.

41. By persuading those customers to implement its products in schools, Seesaw gains virtually unfettered access to the data of the children who attend those schools.

---

[9] *Id.*

[10] Instructure, *The EdTech Top 40: A Look at K-12 EdTech Engagement During the 2023-24 School Year,* available at https://www.instructure.com/resources/research-reports/edtech-top-40-look-k-12-edtech-engagement-during-2023-24-school-year?filled (last accessed May 1. 2025).

[11] *Id.*

42. Seesaw claims that its platform is used by over ten million teachers, students, and family members each month across more than 75 percent of schools in the United States.

43. Seesaw does not publicly disclose the full extent of the data it generates and collects from school-aged children.

44. Seesaw admits that it takes "personal information" from "Data Subjects," which include young students.

45. Seesaw discloses that it collects the following information from and about children:

a. Child's Account Information

i. Student name and/or username;

ii. Email address;

iii. Optional profile picture or avatar;

iv. Data provided by a teacher or school administrator when creating the account or by the students themselves; and

v. Data from third-party authentication services (e.g., Google or Clever) if used by the school.

b. Journal content uploaded by the child:

i. Photos;

ii. Audiovisual content (e.g., from the device's camera, microphone, or photo/video library);

iii. Drawings;

iv. Files;

v. Notes;

vi. Hyperlinks;

vii. "Other ways of documenting student learning"; and

viii. Comments on class posts and student journals (including text and voice recordings).

c. Messages sent or received by the child:

i. Photos;

ii. Messages sent or received by the student, which may include:

a. Text;

b. Audio;

c. Video;

d. Photos;

e. Drawings;

f. Files;

g. Notes;

h. Hyperlinks; and

i. "Other Information."

d. Child's activities:

i. Text instructions;

ii. Voice instructions;

iii. Response examples;

iv. Templates;

v. Activity journals; and

vi. Author profile.

e. Child's communications with Seesaw:

i. Email communications;

ii. Phone communications;

iii. Chat communications; and

iv. Survey responses.

f. Child's information from Google accounts or other third-party sign-in services:

i. Name;

ii. Profile picture;

iii. Email address; and

iv. "Other information (if available)."

g. Device Information and Log Data:

i. Pages visited;

ii. Time spent on the service;

iii. Actions taken (e.g., views, uploads, messages);

iv. "Other similar interaction data";

v. IP Address;

vi. First-party Cookie Identifiers;

vii. Browser Type;

viii. Operating System;

ix. Device Information and Identifiers; and

x. Mobile Carrier.

46. The personal and private information taken from students by Seesaw without effective consent is referred to as the "Stolen Information" herein.

47. The Stolen Information far exceeds what is legally or traditionally characterized as "education records."

48. Even if certain Stolen Information could be characterized as education records, children and their parents retain significant rights over the personal and private information contained in such records.

49. The Stolen Information, including information from and about children under thirteen, far exceeds that reasonably necessary for children to participate in any school activity facilitated by Seesaw in violation of COPPA.

50. Seesaw could design the product it markets and sells to K-6 education institutions to minimize the amount of data it collects from children, but instead it optimizes its product for data extraction.

51. That Seesaw's products are not designed to optimize student privacy is an intentional, self-interested choice that comes at the expense of children's privacy, safety, health, and wellness.

B. Seesaw uses and discloses children's personal and private information for commercial purposes.

52. Seesaw uses and discloses the personal information it generates, extracts, and collects from children for a host of purposes, including commercial purposes.

53. The following elaborates upon some of these uses and disclosures.

1. Seesaw uses and discloses student data to myriad third parties to develop, maintain, and market its own products.

54. Seesaw uses Stolen Information to develop, deliver, maintain, manage, and market its own products.

55. As part of those uses, Seesaw shares Stolen Information with myriad third parties that Seesaw describes as "subprocessors."

56. According to Seesaw, it shares student data with "a small number of third-party service providers in order to operate and improve Seesaw" including "a handful of third-party subprocessors."

57. In fact, Seesaw shares student data with more than thirty (30) so-called subprocessors.

58. Seesaw vaguely describes these entities as "other companies that we share information with to help us do business." It states that "[t]hese companies help us do things like manage our data[.]"

59. Although the quality and quantity of information to which Seesaw grants each of these entities access appears to vary, Seesaw admits that some entities receive access to "everything in Seesaw."

60. As a result, some of the entities with whom Seesaw shares student data gain unrestricted access to the complete range of personal data collected by the platform.

61. Seesaw amends its list of purported subprocessors without notice to parents in violation of COPPA.

62. Seesaw does not adequately describe who those entities are, what those entities do

with student data, what types of student data they collect, how they collect student data, or why student data is shared with those entities.

63. As of the date of this filing, Seesaw's list of "subprocessors," along with a general description of the data shared with each, are as follows:

Entity Name	**How We Use This Subprocessor**	**Data Shared with Entity**
Amazon Web Services	We use Amazon Web Services (AWS) to manage our data centers and the computers that we use to operate Seesaw. All information we collect is stored on computers and databases managed by AWS.	Everything in Seesaw.
Amplitude	We use Amplitude for analytics and reporting in the Seesaw app.	User device information and actions or interactions with the app.
Datadog	We use Datadog for analytics and reporting in the Seesaw app.	User device information and actions or interactions with the app.
Google (Analytics, Firebase, Google Workspace)	We use Google for analytics and reporting as well as for internal documentation.	Analytics and Firebase: Device information, county-level location. Google Workspace: Seesaw teammates collaborate via Google Workspace and may incidentally share limited user data like email address or user IDs of individuals submitting requests and the content of the requests itself (e.g., bug reports, any other help center requests, and data pull requests from teachers and schools).
HighTouch	We use HighTouch to sync data between two other systems.	Teacher and admin name and email address.
Maxio (SaasOptics)	We use Maxio for business tracking.	Admin name and contact information.
Outreach	We use Outreach to send	Admin name and contact

	emails to current and prospective customers.	information.
Quickbooks	We use Quickbooks for financial tracking and for auditing purposes.	Admin emails related to purchase orders.
Salesforce and native apps: Sonar, Tableau, Vicasso	We use Salesforce and its native apps for customer tracking.	Admin name and contact information.
Snowflake	We use Snowflake for Analytics and Reporting	Name and email address.
Stripe	We use Stripe for payment processing.	Admin name and school payment information.
Twilio	We use Twilio to send text messages to Seesaw users about activity in their account.	User phone number (if provided).
Calendly	We use Calendly to schedule customer calls.	Admin name and contact information.
Docusign	We use Docusign to electronically sign contracts.	If you receive a Docusign contract, name, and email address.
Form Assembly	We use Form Assembly to electronically sign contracts.	If you receive a Form Assembly contract, name, and email address.
Gong	We use Gong to record calls, emails, and demos with current and prospective customers.	Admin name, contact information, and call recording if the recipient consents.
LeanData	We use LeanData to improve routing of opportunities for the Sales team.	Admin name and contact information.
Marketo	We use Marketo to manage email campaigns and marketing channels.	Data directly taken from Salesforce.
Slack	We use Slack for internal employee communication.	Seesaw teammates collaborate via Slack and may incidentally share limited user data like email address or user IDs of individuals submitting requests and the content of the requests itself (e.g., bug reports, any other help center requests, and data pull requests from teachers and schools).

Zapier	We use Zapier to communicate between web applications.	Seesaw teammates use Zapier to efficiently manage multiple web applications and may incidentally share limited user data like email address or user IDs of individuals submitting requests and the content of the requests itself (e.g., bug reports, any other help center requests, and data pull requests from teachers and schools).
Ada	We use Ada to provide automated customer support to adults via a chat interface.	If you use our support chatbot, Ada will receive all the information you input. If you submit a support ticket through Ada, Ada will receive your name and email address.
BigMarker	We use BigMarker to host webinars with admins and teachers.	Admin and teacher name and contact information.
Chameleon	Seesaw uses Chameleon to give teachers and admins real-time updates on product updates and provide product tips to help them navigate and utilize the platform.	Limited user data such as role type (teacher or admin); email domain; district, user, and org IDs; and general account data (last seen, date created, etc.).
Chili Piper	We use Chili Piper to help prospective customers navigate the website, drive lead generation, and have live chat conversations to schedule meetings.	The information inputted in the request form- Admin name, email, title, school name and state or country
Thinkific	We use Thinkific to provide Seesaw trainings to teachers.	Teacher name and contact information.
Typeform	We use Typeform to conduct surveys and user research.	Your name and contact information if you are asked to complete a survey. Students do not participate in surveys.
Zendesk	We use Zendesk to operate our internal customer support tools, such as our help center and support ticketing system.	If you submit a support ticket, Zendesk will receive your name, contact information, and the content of your support request. Seesaw takes steps to prevent students from contacting Seesaw support and deletes any support

		requests and associated data students submit to Zendesk.
CookieYes	We use CookieYes to obtain and honor cookie consent preferences on web.seesaw.me.	If you visit Seesaw's website, your IP address.

64. This information has little meaning to the average person. Many key terms are undefined and not readily comprehensible, such as:

a. "analytics and reporting in the Seesaw app";

b. "internal documentation";

c. "business tracking";

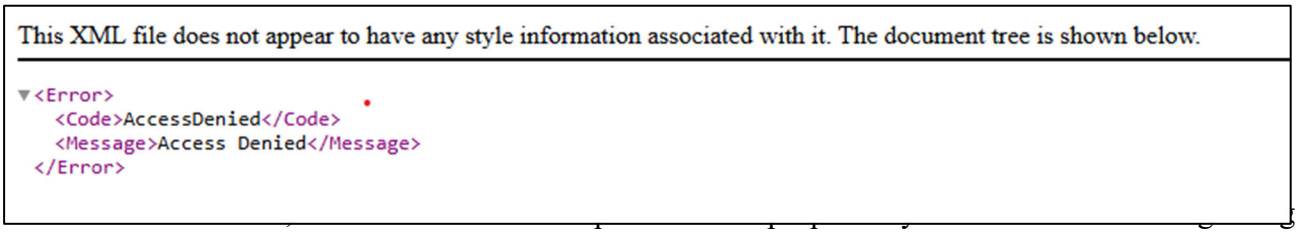
d. "customer tracking"; and

e. "conduct surveys and user research."

65. These disclosures do not adequately notify parents of Seesaw's data practices.

66. Further, Seesaw's disclosure of data to so many entities is especially concerning given that only 20 percent of the security-practice links for each entity on its website are even functional.

67. For example, Seesaw's link to the security practices of Amazon Web Services —which receives "everything in Seesaw"—redirects to the following:



these entities' security practices, 22 are broken.

69. Consequently, parents must undertake a time-consuming and often futile scavenger hunt in an effort to uncover the security practices of dozens of entities and determine whether their child's personal data is at risk.

70. In addition to sharing student data with the above-listed entities, Seesaw purports to grant itself a virtually unlimited right to use student data—including children's names, voices, and

likeness—for its own commercial purposes.

71. In its Terms of Service, Seesaw states that it retains "a royalty-free, sublicensable, transferable, perpetual, irrevocable, worldwide, non-exclusive, license to access, use, host, store, reproduce, modify, publish, list information regarding, translate, process, copy, distribute, perform, export, display, and make derivative works of all User Content, and the names, voice, and/or likeness contained in the User Content, in whole or in part, and in any form, media, or technology, whether now known or hereafter developed, (i) to provide, improve, enhance, develop, maintain and offer products or services; (ii) to prevent or address service, security, support or technical issues; (iii) as required by law; and (iv) as expressly permitted in writing by you."

72. Seesaw further purports to reserve for itself sweeping rights to use "User Content," which includes data "such as profile information, videos, images, music, comments, questions, and other content, data, and/or information[.]" It states that it retains "the right to use, copy, reproduce, store, modify, publish, list information regarding, edit, translate, distribute, syndicate, publicly perform, publicly display . . . and allow other Users to view and access, all such User Content and your name, voice, and likeness as contained in your User Content for the purposes of sharing within your Seesaw Classroom and/or the Community Library, if applicable, and to perform such other actions as described in our Privacy Notice or as authorized by you or the Customer in connection with your use of the Service."

73. Seesaw purports to retain even broader rights over "Usage Data," which includes "information about your computers, mobile devices, systems, and software." It claims that it may use such data for essentially any purpose.

74. In its California Standard Student Data Privacy Agreement ("DPA"), Seesaw further claims to reserve *all* rights to "De-Identified Data" even beyond termination of the DPA and even after any request by the school to return or destroy student data.

75. Seesaw further uses and discloses Stolen Information as follows:

a. as necessary to comply with applicable law;

b. as necessary to respond to a valid legal request, including national security or law enforcement;

c. in the event of a sale of Seesaw;

d. in the event of a sale of certain Seesaw assets;

e. in the event of a merger of Seesaw with another entity;

f. in the event Seesaw reorganizes; or

g. in the event Seesaw declares bankruptcy.

76. Seesaw also purports to reserve for itself a right to transfer children's personal information internationally to "Adequate Jurisdictions" as Seesaw defines that term.

77. Such licenses have significant value.

78. Children do not grant such licenses to private companies to take and use their personal information—without their knowledge or compensation—simply by attending school and using school services as is their legal right and duty.

2. Seesaw discloses student data through data-sharing agreements with its "integration" partners.

79. In addition to those previously described, Seesaw also discloses the personal information it generates, extracts, and takes from young children to a host of other third parties it describes as "integration partners."

80. For example, Seesaw partners with existing EdTech providers through Learning Tools Interoperability ("LTI") integration, allowing students and teachers to integrate Seesaw features directly into the Canvas Learning Management System ("LMS").

81. LTI integration "refers to the process of connecting and enabling communication between various electronic learning ("e-learning") applications and platforms." LTI integration allows an LMS to seamlessly connect with external tools, granting access to student data. This enables students and teachers to access and interact with multiple learning tools directly from the LMS, without needing separate logins for each tool.

82. Additionally, "LTI allows the secure and efficient exchange of data between learning platforms."

83. Seesaw partners with multiple e-learning platforms through LTI integration and has

data-sharing agreements with those platforms. However, the scope of the data shared or provided to these platforms is not publicly accessible.

84. Seesaw partners with "leading edtech providers including popular LMS and SIS platforms . . . ."

85. Some of these partners include the following:

a. **Apple** – Allowing users to use Seesaw on iPad's and add work created in Apple apps like Keynote, Pages, or GarageBand directly into Seesaw portfolios.

b. **D2L** – Providing schools with a way to track student achievements, identify learning gaps, and document progress.

c. **ClassLink** – Allowing for the creation of new classes in Seesaw using existing student data from your SIS, while also enabling the setup of teachers, students, and classes across multiple schools in your district at once.

d. **Clever** – Allowing for the creation of new classes in Seesaw using existing student data from your SIS, while also enabling the setup of teachers, students, and classes across multiple schools in your district at once.

e. **Schoology** – Allowing teachers and students to access Seesaw activities within Schoology.

f. **Canvas** – Allowing teachers and students to access Seesaw activities within Canvas.

g. **Google Classroom and Chromebook**– Allowing for integration with Google Classroom, enabling features such student rostering, assignment of Seesaw activities, and direct uploads from Google Drive to Seesaw.

h. **Microsoft SSO** – Allowing students, families, teachers, and administrators to access Seesaw by using an existing Microsoft account.

i. **Okta** – Allowing teachers and students to sign in with Okta SSO within the Seesaw app or launch the Seesaw app from the Okta user dashboard.

j. **Wonde** – Allow for the creation of new classes in Seesaw using existing student data from your SIS, while also enabling the setup of teachers, students, and classes across multiple schools in your district at once.

86. Seesaw does not publicly fully disclose the data it shares with its integration partners.

87. Its primary value to third-party partners depends on maximizing access to Stolen Information.

88. Data exchanged through these partnerships—including children's personal and private information—enables Seesaw and participating partners to develop, improve, expand, deliver, support, market, and sell their products and services.

89. Third-party partners thus not only receive student data from Seesaw, but they also commercially benefit from such accessing and using such data.

90. Although Seesaw admits to using student data in certain ways that could be lawful if that data was lawfully obtained, those uses are unlawful because Seesaw obtains the data it generates and collects from students through its products without effective consent. In other words, because the information is stolen, there are no legitimate uses of it.

III. Seesaw fails to obtain effective consent for its generation, extraction, use, and disclosure of children's personal and private information.

91. Seesaw fails to obtain effective consent for its sweeping collection and use of children's personal and private information. Specifically, Seesaw fails to (1) provide adequate information to support informed consent, (2) obtain consent from a person with authority to do so, (3) determine whether students' use of its products is voluntary, and (4) provide students and parents with proper consideration in exchange for their agreement to its data practices.

A. Seesaw fails to disclose sufficient information about its data practices to support informed consent.

92. For consent to be effective, Seesaw must explicitly notify users of the specific conduct and practices at issue.

93. Seesaw is required to provide disclosures regarding its data practices so that a reasonable user would understand and know what they were consenting to.

94. Further, before collecting personal information from children under thirteen, Seesaw is also required to provide parents direct notice of its data practices that is "clearly and understandably written, complete," and contains "no unrelated, confusing, or contradictory materials." 15 U.S.C. § 6502; 16 C.F.R. § 312.4.

95. Informed consent is not possible because Seesaw does not provide information regarding its data practices necessary to support informed consent.

96. A reasonable user cannot understand Seesaw's data practices by reviewing Seesaw's disclosures.

97. Seesaw fails to provide information that it discloses (1) the data it collects on students; (2) the ways in which it will use such data; (3) the entities that will have access to such data; and (4) the ways in which those entities will use such data.

98. Seesaw also fails to provide parents of students under thirteen with notice of its data practices that is clearly and understandably written, complete, and contains no unrelated, confusing, or contradictory materials.

99. In fact, a reasonable person may not even definitively determine which disclosures govern students' use of these products. Information relating to Seesaw's data practices and those of its third-party partners are scattered across its sprawling website and others. Such information may be or appears to be found in at least the following locations:

a. Terms of Service (https://seesaw.com/terms-of-service/);
b. End User Terms (https://seesaw.com/end-user-terms/);
c. Service Privacy Policy (https://seesaw.com/service-privacy-policy/);
d. Privacy & Security (https://seesaw.com/privacy-security/);
e. Children's Privacy Policy (https://seesaw.com/childrens-privacy-policy/);
f. California Consumer Privacy Act (https://seesaw.com/california-privacy-act/);
g. COPPA Direct Notice to Schools (https://seesaw.com/coppa-direct-notice-to-schools/)
h. Partnerships (https://seesaw.com/partnerships/);
i. How Seesaw keeps student data safe (https://help.seesaw.me/hc/en-us/articles/203258429-How-Seesaw-keeps-student-data-safe);
j. Subprocessors (https://seesaw.com/subprocessors/);
k. Data Processing Agreement (https://seesaw.com/data-processing-agreement/);
l. Data Privacy Agreements by State (https://help.seesaw.me/hc/en-us/articles/4403250029325-Data-Privacy-Agreements-by-State?);
m. Google Privacy Policy (https://policies.google.com/privacy); and

n. Google APIs Terms of Service (https://developers.google.com/terms).

100. Seesaw also provides children access to myriad third-party services and states that "[i]f you use a third-party service in connection with the service, you are subject to and agree to, and must comply with, the third party's terms and conditions made available via, or agreed in connection with, its services."

101. Thus, even if a parent was notified that their child would be using the Seesaw Platform at school, it would be impossible for that parent to understand Seesaw's data practices as necessary to support their informed consent to those practices on behalf of their child.

102. While Seesaw misleadingly claims it does not sell or rent the data it generates, generates, collects, and uses, it fails to acknowledge the numerous third-party entities with which it shares that data for commercial purposes.

103. No reasonable person may sufficiently understand the extent of Seesaw's and its partners' generation, collection, aggregation, use, and sharing of personal information about and belonging to school-aged children, primarily children under thirteen.

104. Seesaw's disclosures thus fail to meet generally applicable data-privacy standards, as well as the heightened requirements of COPPA.

B. Seesaw does not obtain parental consent to generate, collect, or use children's personal information.

105. Seesaw does not obtain effective consent to generate, collect, or use children's personal and private information.

106. As previously detailed, Seesaw collects data directly from school-aged children through their use of its products. And Seesaw retains, processes, and shares that data and its data-derivative products with a host of third parties for commercial purposes.

107. Consent is effective only if the aggrieved person consented to the particular conduct, or to substantially the same conduct, and if the alleged tortfeasor did not exceed the scope of that consent.

108. Because minors are not legally competent to provide valid, binding consent, the

collection of data from children requires parental consent.

109. In addition to these general standards of consent, COPPA contains a heightened parental-consent requirement that Seesaw must meet before it may collect personal information from children under thirteen. *See* 16 C.F.R. § 312.5. Specifically, COPPA requires that Seesaw "obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented." *Id*. § 312.5(a)(1). Seesaw does not obtain such consent and does not meet any of the exceptions to COPPA's rigorous consent requirement. *Id*. § 312.5(c).

110. Seesaw fails to obtain effective consent from parents for its collection or use of their children's data as described herein, under general consent standards or the heightened COPPA standards.

111. For children under thirteen, Seesaw relies on the school's consent *alone*. In its Service Privacy Policy, it states that Seesaw "rel[ies] on the School to provide appropriate consent for Seesaw to collect personal information directly from a student under 13 for the use and benefit of the School and for no other commercial purpose, as permitted by COPPA."

112. In its COPPA Direct Notice to Schools, Seesaw further states that "[b]y agreeing to [its] Terms of Service and using the Seesaw Services, the School provides consent, on behalf of its Child students' parents or guardians, to Seesaw's collection, use, and disclosure of personal information from and about Children through Services."

113. Schools have no rights or duties under COPPA. Companies are not relieved of their duties under COPPA in the education setting. In fact, schools are not mentioned at all in COPPA.

114. Schools do not own the personal and private information that Seesaw generates about students or extracts directly from students.

115. School administrators are not legal guardians of students.

116. Students have significant privacy and property rights in their own personal and private information.

117. Schools cannot legally consent—in lieu of parents or over parents' objections—to the

collection or use of personal information about and belonging to children by a third party, particularly a privately-owned, for-profit technology company for commercial purposes, even if such collection and use may confer a benefit to schools that is administrative, pedagogical, or otherwise.

118. Schools do not control the collection, storage, or use of student data by Seesaw or any third party to which Seesaw grants access to student data. Indeed, Plaintiffs' school district admitted that it has access to only "data that we send to the companies, not anything the companies create."

119. Students retain significant, legally protected privacy interests in their personal information contained within education records.

120. Seesaw generates and obtains student data in excess of education records.

121. Seesaw generates, obtains, and uses student data more than legitimate educational interests.

122. Seesaw rediscloses personal information to a host of third parties without prior parental knowledge or consent.

123. Schools do not obtain effective parental consent to Seesaw's collection and use of student information as a parent's agent or intermediary, not least because schools lack the information necessary to support informed consent, as described herein.

124. Parents are entitled to be fully informed of the potential benefits and risks that Seesaw's data practices pose to their children. Once fully informed, parents have the right to decide whether to subject their children to those risks in exchange for valuable consideration beyond the education services to which they are already entitled.

125. Seesaw thus collects, uses, and discloses children's personal and private information without obtaining effective consent.

C. FERPA does not relieve Seesaw of its duty to obtain parental consent.

126. Seesaw also states or implies that Seesaw or schools need not obtain parental consent to collect and use student data under FERPA.

127. Under FERPA, schools need not obtain parental consent to disclose education records to a "school official" under narrow circumstances.

128. Seesaw states that it is a signatory to the National Data Privacy Agreement,[12] by which it purports to designate itself a "school official" under FERPA. Under the school-official exception to FERPA's broad prohibition against disclosure of education records, a school may disclose such records to a third party without parental consent if the third party meets FERPA's narrow definition of a "school official." See 34 CFR § 99.31(a)(1). Despite its unilateral designation, Seesaw does not obtain and use student data as contemplated by the school-official exception of FERPA.

129. Schools do not control the maintenance and use of the personal information Seesaw collects from children and their parents, including education records.

130. Seesaw does not only receive students' and parents' personal information from schools: it generates and collects such information directly from students.

131. Seesaw generates and collects personal information in excess of student education records as defined by FERPA.

132. Seesaw generates, collects, and uses data more than legitimate educational interests as contemplated by FERPA. Seesaw rediscloses personal information to a host of third parties without prior parental consent.

133. FERPA thus does not absolve Seesaw or schools of their duty to obtain parental consent before generating, obtaining, using, and disclosing children's personal and private information.

D. Students' use of Seesaw's Platform is not voluntary as it would be necessary to support their or their parents' agreement to Seesaw's data practices.

134. Voluntariness is an essential element of contract formation.

135. A party seeking to prove the existence of a contract must prove that it was entered into voluntarily.

136. California has compulsory education laws.

137. Schools use the Seesaw Platform to support a host of pedagogical, administrative, and

[12] Seesaw has not adopted the most current version of that agreement, which was updated in April 2024. The Student Data Privacy Consortium, *National Data Privacy Agreement,* Apr. 24, 2024, available at https://privacy.a4l.org/national-dpa/ (last accessed May 1, 2025).

other functions.

138. Plaintiffs were not given a choice regarding whether to use Seesaw's Platform at their school.

139. Plaintiffs were not able to opt out from using the Seesaw Platform at school.

140. Even if students theoretically could opt out of using the Seesaw Platform, Seesaw may not place students and their parents in the position of having to choose between their right to privacy and their right to an education or risk compromising their relationship with school personnel. Such inherently coercive circumstances do not support voluntary consent.

141. Because students and parents lack the ability to decline or avoid use of the Seesaw Platform, any purported agreement by them to Seesaw's terms and policies is ineffective.

E. Seesaw does not provide students with sufficient consideration as necessary to support any agreement to Seesaw's data practices.

142. Sufficient consideration, or the legal exchange by parties of something of value, is an essential element of contract formation.

143. A party seeking to prove the existence of a contract must prove that it was supported by sufficient consideration.

144. California has laws guaranteeing children the right to an education.

145. That right includes the right for students to avail themselves of products and services offered by an education institution, which includes essential tools like textbooks and digital learning platforms.

146. Schools use the Seesaw Platform to support a host of pedagogical, administrative, and other education-related functions.

147. Students' use of the Seesaw Platform is thus a part of the education to which they are already legally entitled.

148. Seesaw does not offer students any additional benefit beyond those to which students are already entitled that might constitute sufficient consideration to support any agreement to Seesaw's terms and policies, including those governing Seesaw's data practices.

149. Plaintiffs were provided no additional consideration that might have supported any agreement to Seesaw's data practices.

150. Any purported agreement between Seesaw and students is not supported by the exchange of any new benefit.

151. Without consideration, Seesaw may not establish the existence of any agreement between Seesaw and the students whose information it generates, takes, and uses for commercial purposes or their parents.

IV. Seesaw makes false and misleading statements about its data practices on which it intends the public, school personnel, and parents to rely.

152. Seesaw makes false and misleading statements about its data practices and its commitment to privacy on which it intends the public, schools, and parents to rely.

A. Seesaw falsely states that it prioritizes children's privacy.

153. Seesaw falsely touts its commitment to privacy prominently across its website. On its Privacy and Security webpage, for example, Seesaw states that "[p]rotecting your privacy is fundamental to our mission and business:

154. Seesaw reiterates that false statement in its Service Privacy Policy.

155. In fact, broadly collecting and sharing data is fundamental to Seesaw's mission and

business.

156. In its Data Privacy Agreements, Seesaw falsely states that it "understands the importance of protecting students online, which is why [it has] built privacy, safety, and security into the Seesaw experience."

157. Seesaw's far-reaching data practices are antithetical to student protection. The Seesaw Platform is designed to maximize student data flow and accessibility among its own products as well as third-party products.

158. Seesaw falsely states that it is transparent about its data practices:

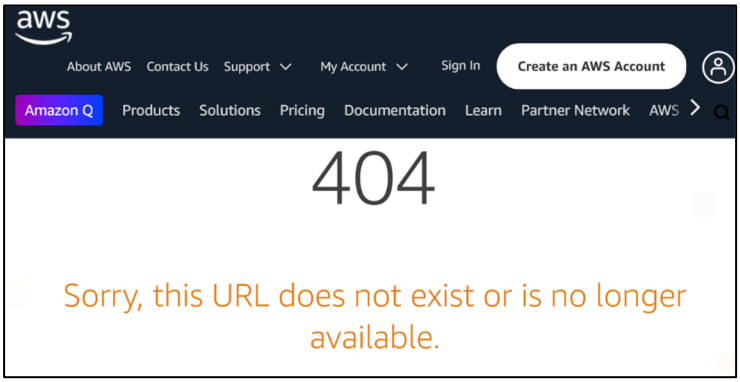
We are transparent about how we collect and handle your personal data

159. But its purported disclosures regarding its data practices are inaccurate and incomplete.

160. For example, Seesaw misleadingly asserts that it only uses a "handful" of subprocessors, defined as "other companies that [it] shares information with to help [it] do business." In reality, the list contains more than thirty (30) entities, at least one of which is granted access to "[e]verything in Seesaw," which may use student data for a variety of commercial purposes.

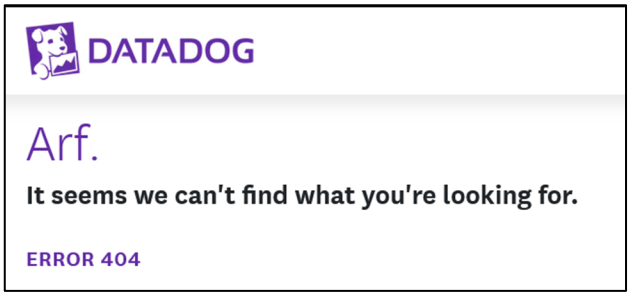
161. Seesaw then purports to link to the privacy policy of each entity. However, of the 31 entities listed, only six linked to the entity's privacy policy. The remaining 25 links were either broken or linked to irrelevant information:

a. Amazon Web Services:



b. Amplitude:

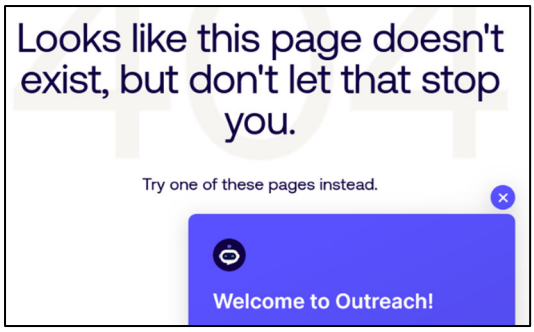
c. Datadog:



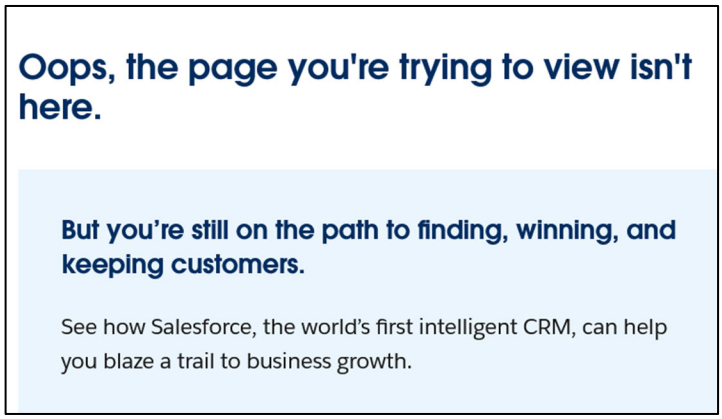
d. HighTouch:

e. SaaSOptics:

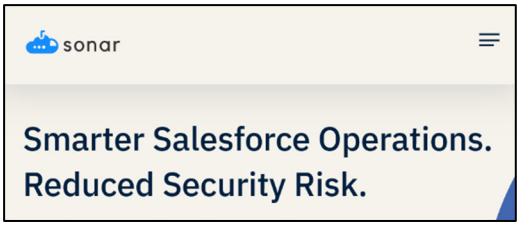
f. Outreach:



g. Salesforce:

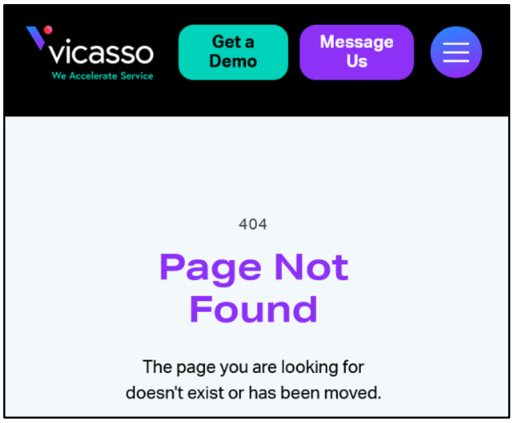


h. Sonar:



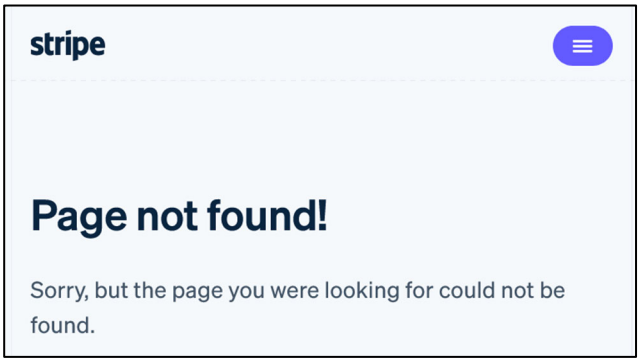
i. Tableau:

j. Vicasso:

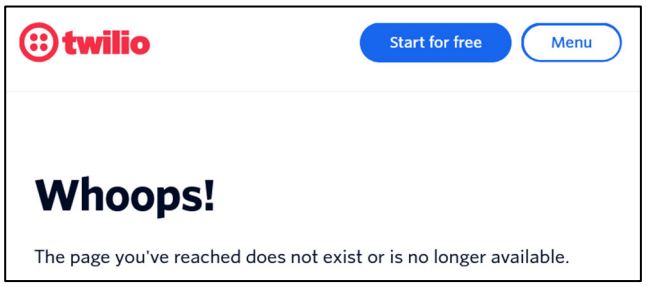


k. Snowflake:

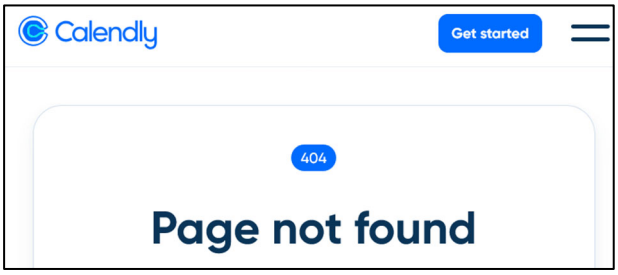
l. Stripe:



m. Twilio

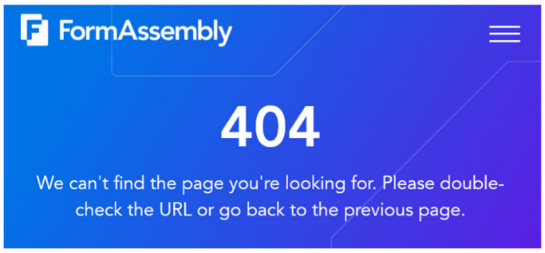


n. Calendly:



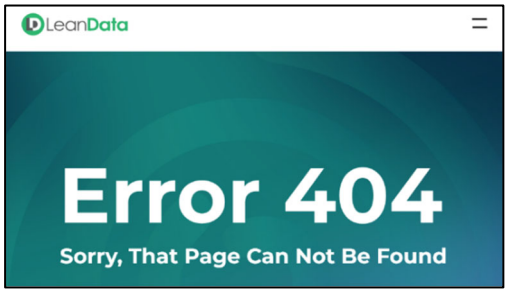
o. DocuSign:

p. Form Assembly:



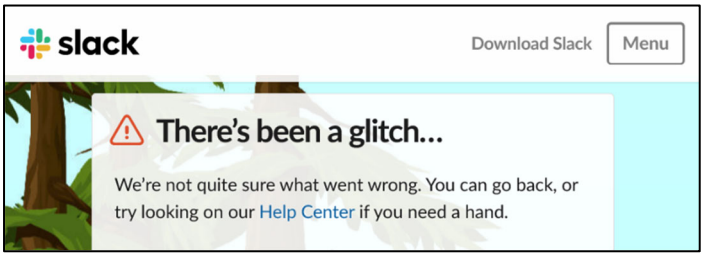
q. Gong:

r. Lean Data:

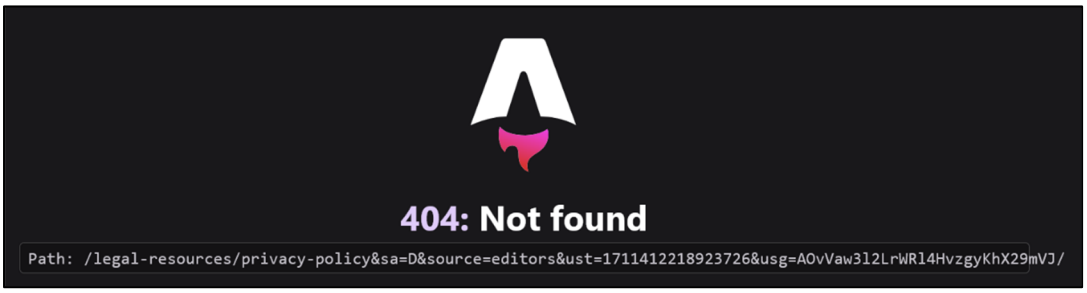


s. Marketo:

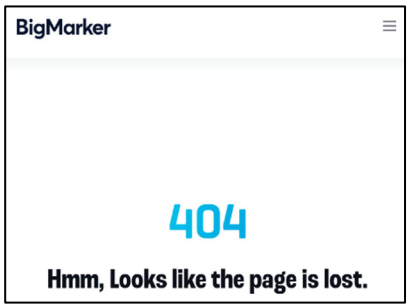
t. Slack:



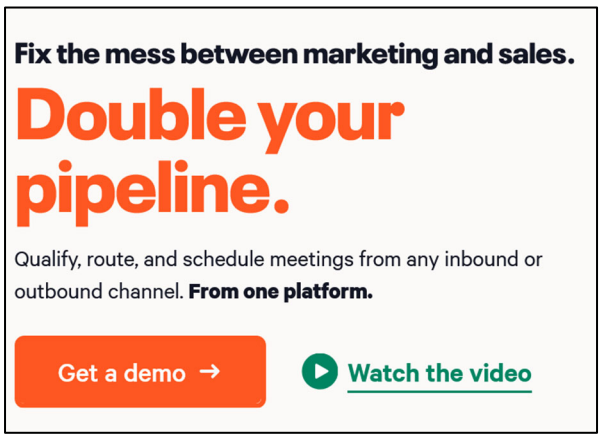
u. Ada:



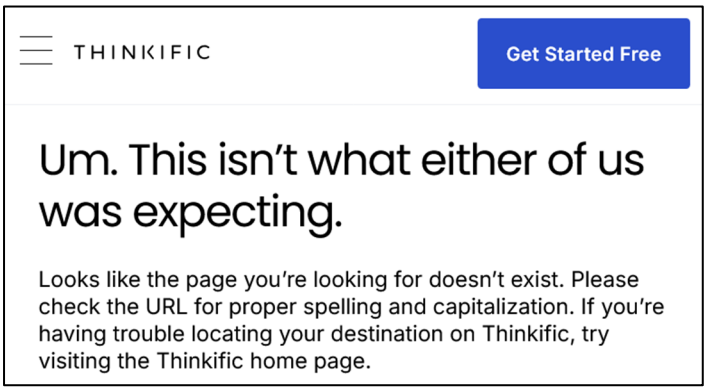
v. BigMarker:



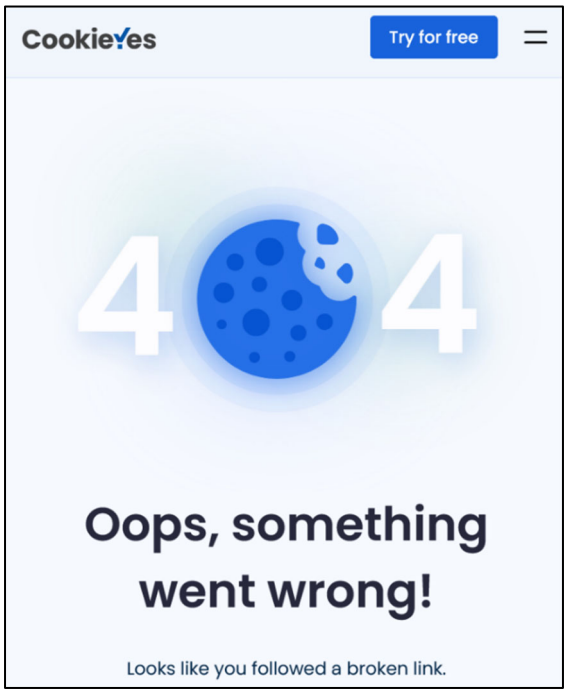
w. Chili Piper:



x. Thinkific:



y. CookieYes:



162. Further, in its "Privacy & Security" webpage, Seesaw misleadingly states that it does not sell or rent information to third parties, while failing to disclose that it makes student information widely available to innumerable third parties for commercial purposes under robust data-sharing agreements.

B. Seesaw falsely states that it may be used in compliance with FERPA.

163. Seesaw falsely and repeatedly states that its services may be used by schools in compliance with FERPA throughout its website.

164. On its "Privacy & Security" webpage, it prominently states that it complies with FERPA:

We never sell your data and comply with FERPA

165. Further, in its data privacy agreements, Seesaw states that "[f]or the purposes of FERPA, [Seesaw] shall be considered a School Official, under the control and direction of the [local

education authority] as it pertains to the use of Student Data" and shall be considered as using student data "with a legitimate educational interest[.]" But Seesaw does not obtain and use student data as contemplated by the school-official exception of FERPA, thus its data practices do not fall within this exception.

166. Schools do not control the maintenance and use of the personal information Seesaw collects from children and their parents, including education records.

167. Seesaw does not only receive students' personal information from schools: it generates and collects such information directly from students.

168. Seesaw generates and collects personal and private information of students in excess of "education records" as defined by FERPA.

169. Seesaw generates, collects, uses, and discloses student data more than legitimate educational interests as contemplated by FERPA.

170. Seesaw rediscloses personal information to a host of third parties without prior parental consent, which is expressly prohibited even under the school-official exception.

C. Seesaw falsely states that it is COPPA compliant.

171. In its Children's Privacy Policy, Seesaw falsely states that it complies with COPPA.

172. In fact, Seesaw violates numerous provisions of COPPA as described herein.

173. Seesaw fails to provide parents complete, understandable notice of its data practices.

174. Seesaw fails to obtain parental consent before taking and using children's personal information.

175. Seesaw falsely states that COPPA requires that Seesaw provide schools direct notice of its data practices. In fact, COPPA requires that Seesaw provide direct notice to parents. COPPA is silent as to schools.

176. Seesaw falsely informs schools that they are authorized to consent to the taking and using of children's data under COPPA. In fact, COPPA requires that Seesaw obtain verified parental consent; lawmakers and regulators have expressly and repeatedly declined to adopt a school exception to the parental-consent requirement.

177. Seesaw collects more personal information from children than is necessary for children to participate in school activities facilitated by Seesaw.

178. Seesaw rediscloses children's personal information to numerous third parties without parental consent.

179. Seesaw falsely states that it "do[es] not require users younger than 13 to disclose more information than is reasonably necessary to use the Services." Seesaw retains children's personal information for longer than is necessary to fulfill the stated purpose for which the information was collected.

D. Seesaw falsely states that it complies with the Student Privacy Pledge

180. Seesaw falsely states that it adheres to the Student Privacy Pledge. The Privacy Pledge contains a number of privacy commitments, including:

a. "We will not collect, maintain, use or share Student PII beyond that needed for authorized educational/school purposes, or as authorized by the parent/student."

b. "We will not sell student PII."

c. "We will not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student."

d. "We will disclose clearly in contracts or privacy policies, including in a manner easy for institutions and parents to find and understand, what types of Student PII we collect, if any, and the purposes for which the information we maintain is used or shared with third parties."

e. "We will incorporate privacy and security when developing or improving our educational products, tools, and services and comply with applicable laws."

181. Seesaw does not adhere to many of the commitments stated in the Privacy Pledge, as described herein.

182. In sum, while Seesaw is committed to creating the appearance of concern for children's privacy and parents' rights, its conduct belies those efforts.

E. Seesaw intends that the public rely on its misrepresentations.

183. Seesaw intends that the public—including school personnel and parents—rely on its statements in determining whether to use its products.

184. Parents rely on these statements either directly or indirectly through their school administrators, who rely on these misrepresentations in deciding to utilize Seesaw's products. If school personnel had not been misled as to Seesaw's data practices, they would not have subjected students—especially young children—to those practices. Schools' use of the Seesaw Platform thus permits an inference that they relied on Seesaw's material, false representations about Seesaw's data practices.

185. Further, these false and misleading statements were likely to mislead and deceive the public and harm the public interest. The public has an interest in protecting children from Seesaw's harmful data practices, especially while attending school and participating in essential school activities, such as completing assignments and communicating with teachers.

V. Seesaw's nonconsensual data practices harm children.

186. Seesaw's surreptitious data practices are not benign. Rather, they harm children in myriad ways that are immediate, long-lasting, substantial, and concealed.

A. Seesaw harms children by invading their privacy.

187. When a person's privacy is invaded, especially a child's privacy, the invasion is the harm.

188. A person's right to privacy begins with protection from having information created about them in the first instance.

189. A person's right to privacy also encompasses their right to control information concerning themselves once created. Loss of such control harms their ability to, among other things, manage and minimize risk.

190. Privacy extends to vital rights such as freedom of thought, freedom from surveillance and coercion, protection of one's reputation, and protection against unreasonable searches and takings.

191. As former FTC Commissioner Noah Joshua Phillips observed, "[t]he United States has a proud tradition of considering and protecting privacy, dating back to the drafting of the

Constitution itself."[13]

192. Seesaw uses Stolen Information in countless ways that infringe upon many time-honored privacy rights of children and their parents.

193. Seesaw's data practices forever wrest from children and their parents' control over children's personal information, including the right to decide whether such information is created in the first place.

194. Seesaw even fails to provide children and parents with an understanding of what information it generated and took, who accessed it, and how it was used.

195. Seesaw generates and collects, for its own commercial benefit, data about public-school children while they use its platform as part of their legally required education. Doing so without parental notice or consent is conduct that is highly offensive to a reasonable person and constitutes an egregious breach of social norms.

B. Seesaw harms children by persistently surveilling them.

196. Seesaw harms children by persistently surveilling, monitoring them while they use its Platform.

197. For instance, Seesaw utilizes services like Google Analytics and Datadog to track "what buttons you click on or what pages you visit."[14] Both services have access to student data.[15]

198. The Seesaw Platform also offers "Progress Monitoring," whereby students' assessment scores, activity completion and proficiency ratings are tracked and recorded.[16]

199. Research has shown that persistent surveillance decreases opportunities for children to exercise autonomy and independence. Persistent surveillance hinders children's development of

---

[13] Noah Joshua Phillips, *Taking Care: The American Approach to Protecting Children's Privacy*, U.S. Federal Trade Commission, Nov. 15, 2018, available at https://www.ftc.gov/system/files/documents/public_statements/1422695/phillips_-_taking_care_11-15-18_0.pdf (last accessed May 1, 2025).

[14] Seesaw, *Service Privacy Policy,* available at https://seesaw.com/service-privacy-policy/ (last accessed May 1, 2025).

[15] Seesaw, *Subprocessors,* available at https://seesaw.com/subprocessors/ (last accessed May 1, 2025).

[16] Seesaw, *All-In-One Platform,* available at https://seesaw.com/all-in-one-platform/ (May 1, 2025).

self-regulation and decision-making that are crucial to aspects of responsibility and self-identity.[17]

200. Continuous surveillance can also increase passivity and self-censorship in children rather than genuine expression, compromising their rights to freedom of thought, conscience, communication, creativity, and speech.[18]

201. Continuous surveillance emphasizes compliance with the current social order instead of the cultivation of identity and dignity.[19]

202. Persistent surveillance at school normalizes surveillance in other areas of life and trains children not to value their own and others' privacy and autonomy.[20]

203. It also normalizes the exploitation of children, their personal information, and their educational development for third-party commercial gain without knowledge, consent, or compensation.[21]

204. The oppressive effect of Seesaw's surveillance practices is proportional to the invisibility and pervasiveness of those practices.[22]

C. Seesaw harms children by compromising the security of their personal and private information.

205. By collecting and storing a child's personal information—and by creating information about her that did not previously exist—Seesaw forever jeopardizes that information by making it vulnerable to a host of data security risks.

206. Rates of cybercrime are steadily rising, including mass data breaches.

207. Schools and school districts have been particularly and increasingly targeted by cybercriminals in recent years, which has resulted in leaks of highly personal and sensitive

[17] Caroline Stockman and Emma Nottingham, *Surveillance Capitalism in Schools: What's the Problem?*, Digital Culture & Education (2022) at 6.

[18] *Id*.

[19] *Id*.

[20] *Id.*

[21] *Id*. at 7.

[22] *Id*. at 3.

information about children, some of which perpetrators have made publicly available.

208. Another major student information system was hacked in December 2024, compromising the personal and private information of tens of millions of students.[23]

209. Exposures like these can have immediate and long-term consequences for children. As explained by one cybersecurity professional, whose son's school was hacked, "It's your future. It's getting into college, getting a job. It's everything."[24]

210. Moreover, once compromised, cybercriminals can exploit various tools—such as messaging features—on EdTech platforms to carry out nefarious activities targeting its users.

211. Seesaw is well aware of the security risks its practices pose to children. In 2022, it experienced this very type of breach when unauthorized actors accessed user accounts and sent an explicit photo through the Seesaw Messages feature.[25] For some users, the Platform automatically displayed the image in the chat.[26] As described by one parent, the compromise of Seesaw's Platform "just shows how vulnerable these systems are."[27]

212. Seesaw's data policies and practices thus unduly compromise the security of children's information. And the resulting harms and risks of harms are exacerbated by the sheer volume of data generated and collected by Seesaw and the number of entities that receive access to it. Once such data is unlawfully obtained, the harms are irreversible.

213. Children's data is further compromised by Seesaw's policy and practice of providing

---

[23] Zack Whittaker, *Malware Stole Internal PowerSchool Passwords From Engineer's Hacked Computer*, TechCrunch, Jan. 17, 2025, available at https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-passwords-from-engineers-hacked-computer/ (last accessed May 1, 2025).

[24] Natasha Singer, *A Cyberattack Illuminates the Shaky State of Student Privacy*, The New York Times, July 31, 2022, available at https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html (last accessed May 1, 2025).

[25] Kevin Collier, *Popular school messaging app hacked to send explicit images to parents,* NBC News, available at https://www.nbcnews.com/tech/security/popular-school-messaging-app-hacked-send-explicit-image-parents-rcna47687 (last accessed May 1, 2025).

[26] *Id.*

[27] Molly Guthrey, *Seesaw, Digital Platform Used by Schools,* EducationWeek, available at https://www.edweek.org/technology/seesaw-digital-platform-used-by-schools-compromised-with-inappropriate-image/2022/09 (last accessed May 1. 2025).

access and otherwise sharing that information with an ever-growing multitude of third parties.

214. In sum, Seesaw's data policies and practices harm families from the moment their personal information is generated and taken by Seesaw. That harm is exacerbated by Seesaw's persistent storage, use, and disclosure of that information.

D. Seesaw harms children by failing to compensate them for their property and labor.

215. Seesaw's data practices also harm students in the form of diminution of the value of their private and personally identifiable data, without compensation.

216. Personal data is now viewed as a form of currency.

217. There has long been a growing consensus that consumers' sensitive and valuable personal information would become the new frontier of financial exploitation.

218. A robust market exists for user data, especially children's personal information. User data has been analogized to the "oil" of the digital economy.[28]

219. Furthermore, most consumers value their data and their privacy. Accordingly, an overwhelming majority engage in efforts to protect their data: 86 percent of United States consumers report caring about data privacy and wanting more control; 79 percent are willing to spend time and money to protect their data; and nearly half have terminated relationships with both online and traditional companies over data-privacy concerns, especially younger consumers.[29]

220. The EdTech market is valued at nearly a quarter of a trillion dollars.[30] The broader market for data, especially for children's personal information, is larger still.

---

[28] *The World's Most Valuable Resource is No Longer Oil, But Data*, The Economist, May 6, 2017, available at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last accessed May 1, 2025).

[29] Cisco, *Consumer Privacy Survey: Building Consumer Confidence Through Transparency and Control* at 5 (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (last accessed May 1, 2025).

[30] Louise Hooper, *et al*., *Problems with Data Governance in UK Schools*, Digital Futures Commission, 5Rights Foundation (2022), https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf (last accessed May 1, 2025).

221. The Stolen Information at issue has significant economic value.[31]

222. Seesaw profits from students by acquiring their sensitive and valuable personal information, which includes far more than mere contact information necessary for obtaining consent, such as name, birth date, and email address.

223. Seesaw then provides access to this data to dozens of third parties for a host of unknown purposes, all without the knowledge of students and their parents.

224. Seesaw further purports to reserve for itself broad, perpetual rights to retain and use students' personal and private information—including a young child's name, voice, and likeness—for its own commercial gain without providing consideration or compensation to them or their parents.

225. Seesaw's actions have thus caused students economic injury.

226. By generating, collecting, using, and disclosing Stolen Information, Seesaw has diminished the value of that information and students' future property interest.

227. Seesaw has also deprived students of their choice whether to participate in the data market at all.

E. Seesaw harms children by forcing them to choose between their right to an education and other fundamental rights.

228. Seesaw forces families into the untenable position of having to choose between their right to an education and other fundamental rights, such as their rights to privacy and property.

229. Recent research shows that nearly 80 percent of adults reported being very or

[31] *See, e.g.*, Brendan Hesse, *Get Paid to Watch Ads in the Brave Web Browser*, Life Hacker, Apr. 26, 2019, available at https://lifehacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279 (last accessed May 1, 2025); *The More You Share, the More You Earn*, Reklaim, available at https://www.reklaimyours.com/how-to-earn (last accessed May 1, 2025); Kevin Mercadante, *10 Apps for Selling Your Data for Cash*, Wallet Hacks, Nov. 18, 2023, available at https://wallethacks.com/apps-for-selling-your-data/ (last accessed April 4, 2025); *Facebook Launches App That Will Pay Users For Their Data*, The Guardian, June 11, 2019, https://www.theguardian.com/technology/2019/jun/11/facebook-user-data-app-privacy-study (last accessed May 1, 2025).

somewhat concerned about how companies use data collected about adults,[32] and the number of those concerned about their online privacy is growing quickly.

230. Protective behaviors are on the rise, with 87 percent of adults in the United States using at least one privacy- or security-protecting tool online.[33]

231. An even greater percentage of parents value protecting their children's personal data, including their identity (90%), location (88%), health data (87%), age (85%), school records (85%), and browsing history (84%).[34]

232. By inserting itself between schools and families, Seesaw has driven a wedge between school personnel and parents, leaving parents reluctant to press their schools for information regarding Seesaw's data practices or request that their children be alternatively accommodated.

233. Parents fear becoming adversarial with their children's schools and the possible repercussions they or their children might suffer if they are perceived as difficult or meddlesome, including stigmatization or retaliation by school personnel. Seesaw has thus chilled parental efforts to inquire and object to its data practices.

234. Children and their parents are particularly vulnerable and disempowered to protect themselves against Seesaw's policies and practices.

235. Seesaw should not be permitted to use schools as a shield against parent inquiry and concern. Rather, Seesaw should be made to account for its data practices directly to the people adversely affected by them.

236. As such, Seesaw forces children and parents to choose between equal access to

---

[32] Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, Nov. 15, 2019, available at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last accessed May 1, 2025).

[33] Stephanie Liu, *US Consumer Privacy Attitudes In 2022*, Forrester, Sept. 28, 2022, available at https://www.forrester.com/blogs/us-consumer-privacy-attitudes-in-2022/ (last accessed May 1, 2025).

[34] *Polling Memo: Parents' Views on Children's Digital Privacy and Safety*, Trusted Future (2022), available at https://trustedfuture.org/childrens-digital-privacy-and-safety/ (last accessed May 1, 2025).

education on one hand, and other basic rights, such as rights to privacy and property, on the other.

F. Seesaw's nonconsensual data practices are unfair and unlawful.

237. Seesaw has realized considerable profit through collection and analysis of children's personal information—without effective knowledge or consent—and without compensating them for actively and passively providing that information.

238. This one-sided arrangement—whereby Seesaw earns vast revenues each year from the personal information of children and their parents gathered through the compelled use of Seesaw products, and all children and parents receive in return is an education to which they are already legally entitled—is particularly unjust given the core philanthropic purpose and compulsory nature of receiving an education.

239. Through its false representations and surreptitious data practices, Seesaw is unjustly enriching itself at the cost of children's privacy, security, and autonomy, when children would otherwise have the ability to choose how they would monetize their own data—or decide not to. Young children should not be made to bear these risks and harms for the benefit of a private, for-profit corporation.

VI. Plaintiff-specific allegations

A. Plaintiffs used the Seesaw Platform, which generated, collected, used, and disclosed their personal and private information.

240. Plaintiffs used the Seesaw Platform.

241. Plaintiffs' use of the Seesaw Platform was mandatory.

242. Plaintiffs were unable to opt out of using the Seesaw Platform.

243. Seesaw obtained substantial personal, private, and sensitive information from Plaintiffs.

244. Such data includes personally identifying information, such as name, birthday, grade, email address, "student unique identifier"; school- and class-related information; and Platform-usage data; such as login time and location; device data; numerous photos and videos of Plaintiff children in and around their school, taken of themselves and submitted by school personnel; student-created

content, such as artwork, essays, journal entries, and homework assignments; and hundreds of data points that were indecipherable.

245. In one video take of M.C. 1, she presented to her class details about herself, such as her name, age, where she lives, her friends, her favorite things, and what she wants to be when she grows up, with a large poster visual aid on which those details were written alongside photos of herself and her family.

246. One assignment submitted by M.C. 2 was entitled "Emotions by [M.C. 2]" which listed various emotions with corresponding images of the young boy.

247. The data produced also included extensive, personal information belonging to children other than M.C. 1 and M.C. 2.

248. This information dates back to January 2023—more than two years after Plaintiff Reisberg requested it from Seesaw, which was months after she had pulled her children from the district.

249. The data produced by Seesaw far exceeded that to which the school had access.

250. Seesaw processes and uses information generated, uploaded, or stored in Seesaw databases, including data and information about and belonging to Plaintiffs, for commercial purposes.

251. Seesaw uses this information to develop, improve, and market its products and other commercial purposes.

252. Seesaw uses Plaintiffs' data either that it generated and took from them directly or that it obtained from Plaintiffs' school to develop, maintain, improve, and market its products, which it sells to Plaintiffs' school district.

253. Seesaw has provided third parties personally identifying data belonging to Plaintiffs for commercial purposes, including identification, advertising, targeting, influencing, and decision-making purposes.

254. Seesaw has enabled third parties to directly collect Plaintiffs' personal information.

B. Plaintiffs never consented to Seesaw's generation, collection, and use of their personal and private information.

255. Plaintiffs did not provide effective, informed, voluntary, and ongoing consent to Seesaw's collection and use of their personal and private information for any purpose, let alone commercial purposes.

256. Seesaw never notified Plaintiff Reisberg that her minor children were using the Seesaw Platform, either generally or in compliance with the heightened notice requirements of COPPA.

257. Plaintiffs were never provided material terms regarding Seesaw's data practices, such as what of their personal information that Seesaw is collecting, how it is used, who else can access and has accessed it, or the risks of harm those practices pose to Plaintiffs.

258. Only after (1) Seesaw had collected substantial data belonging to Plaintiff Reisberg's children and (2) Plaintiff Reisberg demanded to review the data Seesaw had collected about her children did Seesaw provide her access to such data.

259. Before releasing her children's data to Plaintiff Reisberg, Seesaw verified her identity as the children's parents through the school, thereby demonstrating that it would have been possible for Seesaw to have obtained her verified consent *before* subjecting her children to its data practices—it simply chose not to.

260. Any purported consent was not informed, was not provided by a person with proper authority, was not voluntary, was not supported by adequate consideration, and was not commensurate with the level of Seesaw's surveillance and profiteering.

C. Plaintiffs were harmed by Seesaw's collection and use of their data.

261. Seesaw's data practices harmed Plaintiffs in several material ways.

262. At minimum, by collecting and retaining minor Plaintiffs' personal and private information, Seesaw compromised the security of that information.

263. Seesaw harmed Plaintiffs by invading their privacy.

264. Seesaw's data practices further compromised Plaintiffs' relationships with various

school administrators, faculty, and staff.

265. Seesaw harmed Plaintiffs by diminishing the value of their data.

266. Seesaw harmed Plaintiffs by denying them control over their own data.

267. Seesaw harmed Plaintiffs by subjecting them to unfair, deceptive practices that have prevented them from understanding the full extent of how they may have been harmed by those practices.

268. Seesaw harmed Plaintiffs by failing to compensate them for their property or labor, which it has used to fuel its highly lucrative business.

D. Plaintiff Reisberg is a long-time advocate for children and parents.

269. Plaintiff Reisberg understands the many harms that data collection and use by private companies for commercial purposes pose to children, including her own children.

270. Plaintiff Reisberg has advocated for online safety and the digital rights of children and parents for years, and has worked to educate parents everywhere about the dangers that data-extractive platforms pose to children.

271. Plaintiff Reisberg was ultimately forced to withdraw her children from their school district to protect their privacy and wellbeing from data-extractive platforms such as Seesaw.

272. Plaintiff Reisberg is now turning to the courts to protect her children and other children from the exploitative practices described herein.

CLASS ACTION ALLEGATIONS

273. This is a class action pursuant to California Code of Civil Procedure section 382 on behalf of the following Class:

> All persons in California who attend or attended a K-12 school that used the Seesaw Platform.

274. Excluded from the Class are: (1) the Court (including any Judge or Magistrate presiding over this action and any members of their chambers and families); (2) Defendant, its subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them have a controlling interest and its officers, directors, employees, affiliates, or legal representatives;

and (3) the legal representatives, successors, and assigns of any such excluded person.

275. **Ascertainability**: Membership of the Class is defined based on objective criteria and individual members will be identifiable from Seesaw's records, including from Seesaw's massive data storage. Based on information readily accessible to it, Seesaw can identify members of the Class who have used Seesaw's products.

276. **Numerosity**: Members of the Class are so numerous that joinder of all members is impracticable. The exact size of the Class and the identities of Class members can be determined through Seesaw's records.

277. **Typicality**: Plaintiffs' claims are typical of the claims of other Class members, as all members of the Classes were uniformly affected by Seesaw's wrongful conduct in violation of federal and state law as complained of herein.

278. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the members of the Classes and have retained counsel that is competent and experienced in class action litigation, including nationwide class actions and class actions involving privacy violations. Plaintiffs and their counsel have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class members. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so.

279. **Commonality**: Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Common questions for the Classes include, but are not limited to, the following:

a. Whether Seesaw led Plaintiffs and Class members to believe, either directly or through school personnel, that their data and their privacy would be protected;

b. Whether Seesaw represented that Plaintiffs and Class members could control what data was intercepted, received, or collected by Seesaw;

c. Whether Seesaw actually failed to protect the data and privacy of Plaintiffs and Class members;

d. Whether Seesaw actually intercepted, received, or collected data from Plaintiffs and Class members;

e. Whether Seesaw failed to obtain informed and voluntary consent to collect data from

Plaintiffs and Class members;

f. Whether Seesaw misrepresented to have proper consent to collect data from Plaintiffs and Class members;

g. Whether Seesaw practice of intercepting, receiving, or collecting data from Plaintiffs and Class members violated state privacy laws;

h. Whether Seesaw's practice of intercepting, receiving, or collecting data from Plaintiffs and Class members violated anti-wiretapping laws;

i. Whether Seesaw's practice of intercepting, receiving, or collecting data from Plaintiffs and Class members violated any other state tort laws;

j. Whether Seesaw mispresented its compliance with various state and federal data privacy laws;

k. Whether Seesaw's misrepresentation deceived Plaintiffs and Class members;

l. Whether Plaintiffs and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

m. Whether Plaintiffs and Class members have sustained damages as a result of Seesaw's conduct and, if so, what is the appropriate measure of damages or restitution.

280. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of a single adjudication, economies of scale and comprehensive supervision by a single, able court. Furthermore, as the damages individual Class members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

281. **California law applies to all Class members**: California's substantive laws apply to every Plaintiff and member of the Class, regardless of where in the United States the Class member resides because Plaintiffs' and Class members' injuries emanate from Seesaw's actions in California. Upon information and belief, each actionable decision related to the creation, implementation, maintenance, monetization, and concealment of the data-harvesting scheme in the United States was

made from Seesaw's California headquarters by its respective executives and employees located in California. Further, Seesaw's own Terms of Service and End User Terms of Service—although not binding against Plaintiffs and Class members—explicitly require application of California law to all disputes relating to use of the service. Its Terms of Service state "that the Services will be deemed solely based in the State of California" and requires that users "consent to the exclusive jurisdiction and venue of the federal courts located in San Francisco, California in all disputes arising out of or relating to the use of the Services or the Agreement[.]" Its Terms further state that "these Terms will be governed by the internal substantive laws of the State of California, without respect to its conflict of laws principles." Its End User Terms of Service similarly state that, "[t]o the maximum extent permitted by law, these Terms will be governed by the internal substantive laws of the State of California, without respect to its conflict of laws principles." By choosing California law for the resolution of disputes covered by its Terms of Service, Seesaw concedes that it is appropriate for this Court to apply California law to the instant dispute to Plaintiffs and all Class members. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and Class members under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the United States' Constitution. Further, the locus of the wrongdoing occurred in California. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiffs and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Seesaw's decision to reside in California, avail itself of California's laws, and engage in the challenged conduct from and emanating out of California renders the application of California law to the claims herein constitutionally permissible. The application of California laws to Plaintiffs and the Classes is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Classes and California has the greatest interest in applying its laws here.

282. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or

otherwise.

CAUSES OF ACTION

Count I: Violation of the California Invasion of Privacy Act ("CIPA") Cal. Penal Code §§ 631, 632

283. Plaintiffs incorporate by reference paragraphs 1 through 282 as though fully set forth herein.

284. CIPA is codified at California Penal Code sections 630–638. The Act begins with its statement of purpose in California Penal Code section 630:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

285. California Penal Code section 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars[.]

286. California Penal Code section 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars[.]

287. Under either section of CIPA, a defendant must show it had the consent of all parties to a communication.

288. Seesaw has its principal place of business in California; it designed, contrived, and effectuated its scheme to track users from California; and has adopted California substantive law to govern its relationship with its users.

289. Seesaw's non-consensual monitoring of Plaintiffs' and Class members' internet communications was without authorization and consent from Plaintiffs and Class members. The interception by Seesaw in the aforementioned circumstances was unlawful and tortious.

290. The following items constitute machines, instruments, or contrivances under CIPA, and even if they do not, Seesaw's deliberate and purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The computer code and programs Seesaw used to track Plaintiffs' and Class members' communications;

b. Plaintiffs' and Class members' browsers and mobile applications;

c. Plaintiffs' and Class members' computing and mobile devices;

d. Seesaw's servers; and

e. The computer codes and programs used by Seesaw to effectuate its monitoring and interception of Plaintiffs' and Class members' communications.

291. The data collected by Seesaw constituted "confidential communications" as that term is used in section 632, because Plaintiffs and Class members had objectively reasonable expectations of privacy in their devices and activity.

292. Seesaw aided and abetted numerous third parties (as described above) in unlawfully intercepting protected communications belonging to Plaintiffs and Class members.

293. Plaintiffs and Class members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

294. Pursuant to California Penal Code section 637.2, Plaintiffs and Class members have

been injured by the violations of California Penal Code sections 631 and 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

Count II: Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code §§ 502, *et seq*.

295. Plaintiffs incorporate by reference paragraphs 1 through 282 as though fully set forth herein.

296. California Penal Code section 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

297. Seesaw violated California Penal Code section 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiffs' and Class members' data.

298. Seesaw effectively charged Plaintiffs and Class members and was enriched by acquiring their sensitive and valuable personal information without permission and using it for Seesaw's own financial benefit to advance its business interests. Plaintiffs and Class members retain a stake in the profits that Seesaw earned from the misuses of their activity and personally identifiable information because, under the circumstances, it is unjust for Seesaw to retain those profits.

299. Seesaw accessed, copied, took, analyzed, and used from Plaintiffs' and Class members' computers in and from the State of California, where Seesaw: (1) has its principal place of business; (2) upon information and belief used servers that provided communication links between Plaintiffs' and Class members' computers and Seesaw, which allowed Seesaw to access and obtain their data; and (3) Seesaw's Terms of Service mandate that the provision of Seesaw's service is "deemed solely based in the State of California" thus foreclosing any suggestion that the service is based anywhere else. Accordingly, Seesaw caused the access of their computers from California and is therefore deemed to have accessed their computers in California.

300. As a direct and proximate result of Seesaw's unlawful conduct within the meaning of California Penal Code section 502, Seesaw has caused loss to Plaintiffs and Class members and has

been unjustly enriched in an amount to be proven at trial.

301. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

302. Plaintiffs and Class members are entitled to punitive or exemplary damages pursuant to California Penal Code section 502(e)(4) because Seesaw's violations were willful and, upon information and belief, Seesaw is guilty of oppression or malice as defined by California Civil Code section 3294.

303. Plaintiffs and Class members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code section 502(e).

Count III: Violation of California's Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.

304. Plaintiffs incorporate by reference paragraphs 1 through 282 as though fully set forth herein.

305. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200 (UCL). By engaging in the practices aforementioned, Seesaw has violated the UCL.

306. A plaintiff may pursue a claim under the UCL through any or all of three prongs: the unlawful prong, the unfair prong, or the fraudulent prong.

307. Seesaw's conduct violated letter and purpose of these laws, which protect property, economic and privacy interests and prohibit unauthorized disclosure and collection of private communications and personal information.

308. Seesaw's unfair acts and practices include its violation of property, economic, and privacy interests protected by federal and state laws.

309. To establish liability under the "unfair" prong, Plaintiffs and Class members need not establish that these statutes were actually violated, although the allegations herein establish that they were. The foregoing allegations are tethered to underlying constitutional, statutory, or regulatory

provisions; describe practices that are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers; and show that negative impact of Seesaw's practices on school-aged children and their parents far outweighs the reasons, justifications, and motives of Seesaw.

310. The foregoing allegations establish liability under the "unlawful" prong, as they show that Seesaw violated an array of state and federal laws protecting privacy and property.

311. The foregoing allegations also establish liability under the "fraudulent" prong, as Seesaw's false and misleading representations and omissions were material, and they were likely to and did mislead some members of the public and caused harm to the public interest. They also misled parents, whether directly or indirectly through school personnel.

312. Plaintiffs and Class members have suffered injury-in-fact, including the loss of money and property as a result of Seesaw's unfair and unlawful practices, to wit, the unauthorized disclosure and taking of their personal information which has value as demonstrated by its use and sale by Seesaw. Plaintiffs and Class members have suffered harm in the form of diminution of the value of their private and personally identifiable data and content.

313. Seesaw's actions caused damage to and loss of Plaintiffs' and Class members' property right to control the dissemination and use of their personal information and communications.

314. Seesaw reaped unjust profits and revenues in violation of the UCL. This includes Seesaw's profits and revenues from their targeted advertising and improvements of Seesaw's other products. Plaintiffs and the Class seek restitution and disgorgement of these unjust profits and revenues.

Count IV: Invasion of Privacy—California Constitution

315. Plaintiffs incorporate by reference paragraphs 1 through 282 as though fully set forth herein.

316. California's constitution creates a right of action against private entities such as Seesaw that are headquartered in and do business in the state of California.

317. Plaintiffs' and Class members' expectation of privacy is deeply enshrined in California's Constitution. Article I, section 1 of the California Constitution provides: "All people are

by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property and pursuing and obtaining safety, happiness, and privacy." The phrase "and privacy" was added by the "Privacy Initiative" adopted by California voters in 1972.

318. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.

319. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Seesaw.

320. A California constitutional privacy claim requires an invasion of: (1) a legally protected privacy interest; (2) where plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

321. As described herein, Seesaw has intruded upon the following legally protected privacy interests:

a. The California Constitution, which guarantees a right to privacy;

b. CIPA; and

c. California common-law rights to privacy.

322. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances in that Plaintiffs and Class members could not reasonably expect that Seesaw would commit acts in violation of state civil and criminal laws.

323. Seesaw's actions constituted a serious invasion of privacy in that it:

a. Violated laws, including the California Invasion of Privacy Act;

b. Invaded the privacy rights of Plaintiffs and Class members without their consent;

c. Constituted an unauthorized taking of valuable information from Plaintiffs and Class members through deceit;

d. Further violated Plaintiffs' and Class members' reasonable expectation of privacy via Seesaw's review, analysis, and subsequent uses of Plaintiffs' and Class members' activity that was considered sensitive and confidential.

324. Committing these acts against Plaintiffs and Class members alike constitutes an egregious breach of social norms that is highly offensive.

325. Seesaw's surreptitious and unauthorized monitoring of Plaintiffs' and Class members' activity constitutes an egregious breach of social norms that is highly offensive, particularly given that its products and services were represented as tools to assist with the educations of young children.

326. Taking this information through deceit is highly offensive behavior, and Seesaw lacked any legitimate business interest in monitoring Plaintiffs and Class members without their consent.

327. Plaintiffs and Class members have been damaged by Seesaw's invasion of their privacy and are entitled to just compensation and injunctive relief.

Count V: Invasion of Privacy—Public Disclosure of Private Facts

328. Plaintiffs incorporate by reference paragraphs 1 through 282 as though fully set forth herein.

329. California recognizes the tort of invasion of privacy by public disclosure of private facts, the elements of which are: (1) the disclosure of the private facts must be a public disclosure and not a private one; (2) the facts disclosed to the public must be private facts, and not public ones; (3) the matter made public must be one that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities.

330. Seesaw disclosed Plaintiffs' and Class members' personal information to its vast network of partners, as described herein. The recipients of Plaintiffs' and Class members' personal information because of Seesaw's disclosures are so numerous that they amount to public disclosures.

331. Moreover, Seesaw's creation and disclosure of intimate digital dossiers containing

Plaintiffs' and Class members' personal information further constitutes public disclosures of that information.

332. The contents of the personal information that Seesaw publicly disclosed is highly personal and not otherwise public knowledge, including education records to include highly sensitive grades, disciplinary records, health records, mental health records, behavioral information, and other highly sensitive information described in this complaint. Seesaw's disclosure of this information would be highly offensive and objectionable to a reasonable person of ordinary sensibilities.

333. As described herein, Seesaw has knowingly intruded upon the legally protected privacy interests in violation of:

a. COPPA;

b. CIPA;

c. CDAFA;

d. The California Constitution, which guarantees a right to privacy;

e. Common-law right to privacy; and

f. Common-law intrusion upon seclusion.

334. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances in that Plaintiffs and Class members could not reasonably expect that Seesaw would commit acts in violation of federal and state civil and criminal laws.

335. Seesaw's actions constituted a serious invasion of privacy in that it:

a. Violated laws, including COPPA, CIPA, and CDAFA;

b. Invaded the privacy rights of Plaintiffs and Class members without their knowledge or consent, including the rights of school-aged children;

c. Constituted an unauthorized taking of valuable information from Plaintiffs and Class members through deceit; and

d. Further violated Plaintiffs' and Class members' reasonable expectation of privacy via Seesaw's review, analysis, and subsequent uses of Plaintiffs' and Class members' activity that was considered sensitive and confidential.

336. Committing these acts against Plaintiffs and Class members alike constitutes an

egregious breach of social norms that is highly offensive, particularly given Seesaw's specific targeting of school-aged children for data extraction and exploitation in a compulsory setting.

337. Seesaw's surreptitious and unauthorized monitoring of Plaintiffs' and Class members' activity constitutes an egregious breach of social norms that is highly offensive, particularly given that Seesaw's K-6-marketed products were represented as tools to assist with the education of children.

338. Taking this information through deceit is highly offensive behavior, and Seesaw lacked any legitimate business interest in monitoring Plaintiffs and Class members without their consent.

339. Plaintiffs and Class members have been damaged by Seesaw's invasion of their privacy and are entitled to just compensation and injunctive relief.

Count VI: Intrusion Upon Seclusion

340. Plaintiffs incorporate by reference paragraphs 1 through 282 as though fully set forth herein.

341. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

342. In carrying out its scheme to conscript parents and their children into the Seesaw Product ecosystem to enable Seesaw to track and intercept Plaintiffs' and Class members' communications in violation of its own privacy promises, Seesaw intentionally intruded upon Plaintiffs' and Class members' solitude or seclusion in that it effectively placed itself in the middle of conversations to which it was not an authorized party.

343. Seesaw's monitoring and interception were not authorized by Plaintiffs and Class members.

344. Seesaw's intentional intrusion into their internet communications and their computing devices and web-browsers was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

345. The taking of personally identifiable information from children through deceit is highly offensive behavior.

346. Seesaw's continued collection of data after Plaintiffs and Class members navigated away from Seesaw's websites and to different and unrelated websites is highly offensive behavior as that collection has no bearing on the application of Seesaw's products to children's education.

347. Wiretapping and surreptitious recording of communications is highly offensive behavior.

348. Public polling on internet monitoring has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is further heightened when children are using the internet.

349. Plaintiffs and Class members have been damaged by Seesaw's invasion of their privacy and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet monitoring.

Count VII: Unjust Enrichment

350. Plaintiffs incorporate by reference paragraphs 1 through 282 as though fully set forth herein.

351. Seesaw has unjustly received benefits at the expense of Plaintiffs and Class members.

352. Seesaw acquired and compromised the security of troves of personal data that rightfully belong to Plaintiffs and Class members without valid consent through intentionally deceptive practices conducted in connection with consumers' use of Seesaw sites and products.

353. Seesaw has derived profits and other tangible benefits from its collection of Stolen Information, without which Seesaw could not as effectively have grown its business, acquired numerous other tangible and intangible assets, developed other products, and supported myriad data-sharing agreements.

354. Seesaw has also directly and substantially profited from its generation, storage, aggregation, use, and disclosures of Plaintiffs' and Class members' data. Indeed, Plaintiffs' and Class members' data is the fuel that powers Seesaw's products.

355. These benefits were the expected result of Seesaw acting in its pecuniary interests at the expense of children and their parents.

356. In exchange for these benefits to Seesaw, Plaintiffs and Class members received nothing more than education services to which they were already entitled.

357. Seesaw did not and made no efforts to determine whether Plaintiffs' and Class Members' use of its Products in compulsory K-6 environments was voluntary.

358. In order to enrich itself, Seesaw deprived Plaintiffs and Class members of their property, security, privacy, and autonomy.

359. Seesaw harmed Plaintiffs and Class members by, among other harms, subjecting them to commercial manipulation and continuous surveillance; invading their privacy; forcing them to choose between their right to an education and other fundamental rights; and failing to compensate them for their property and labor.

360. Plaintiffs and Class members did not provide their consent to Seesaw taking their information and using it for Seesaw's commercial gain.

361. There is no justification for Seesaw's enrichment. It would be inequitable, unconscionable, and unjust for Seesaw to be permitted to retain these benefits because the benefits were procured because of and by means of their wrongful conduct.

362. Plaintiffs and Class members seek an order compelling Seesaw to disgorge the profits and other benefits it has unjustly obtained.

363. Plaintiffs and Class members are entitled to restitution of the benefits Seesaw unjustly retained and/or any amounts necessary to return Plaintiffs and Class members to the position they occupied prior to dealing with Seesaw.

RELIEF REQUESTED

WHEREFORE, Plaintiffs respectfully request the Court enter judgment in their favor and against Seesaw as follows:

a. An award of damages, including actual, compensatory, general, special, incidental, consequential, and punitive damages, in an amount to be determined at trial;

b. Injunctive, declaratory, and other equitable relief as is appropriate;

c. Pre- and post-judgment interest to the extent provided by law;

d. Attorneys' fees to the extent provided by law;

e. Costs to the extent provided by law; and

f. Such other relief the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial for all claims so triable.

Dated: May 8, 2025

Respectfully submitted,

By: _____

Matthew J. Langley (Bar No. 342846)
matt@almeidalawgroup.com
ALMEIDA LAW GROUP
849 W. Webster Avenue
Chicago, IL 60614
Tel.: (773) 554-9354

Julie U. Liddell*
julie.liddell@edtech.law
W. Andrew Liddell*
andrew.liddell@edtech.law
EDTECH LAW CENTER PLLC
P.O. Box 300488
Austin, Texas 78705
Tel.: (737) 351-5855

David J. George*
DGeorge@4-Justice.com
George Feldman McDonald, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Tel.: (561) 232-6002
Fax: (888) 421-4173

Lori G. Feldman*
LFeldman@4-justice.com
Michael Liskow*
MLiskow@4-Justice.com
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel.: (718) 878-6433
Fax: (888) 421-4173

* *pro hac vice* forthcoming

Counsel for Plaintiffs & the Proposed Class