Melisa A. Rosadini-Knott
(California Bar No. 316369)
PEIFFER WOLF CARR KANE CONWAY & WISE LLP
3435 Wilshire Blvd., Ste. 1400
Los Angeles, CA 90010-1923
323-982-4109
mrosadini@peifferwolf.com

[*additional counsel listed on signature page*]

Counsel for Plaintiffs and the Proposed Classes

** pro hac vice forthcoming*

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

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

JASMINE HERNANDEZ-SILVA and MICHAEL SILVA, on behalf of their minor children M.C. 1 and M.C. 2, and HEIDI SAAS, on behalf of her minor child M.C. 3, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

INSTRUCTURE, INC.,

Defendant.

Civ. No.

CLASS ACTION COMPLAINT:

1. 42 U.S.C. § 1983 – 4TH AMENDMENT
2. 42 U.S.C. § 1983 – 14TH AMENDMENT
3. THE CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE §§ 631, 632
4. THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CAL. PENAL CODE §§ 502
5. CALIFORNIA'S UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE § 17200
6. CAL. CIV. CODE § 52.1
7. INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
8. INVASION OF PRIVACY—INTRUSION UPON SECLUSION
9. UNJUST ENRICHMENT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

"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, 2014

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

- Michael Moe, EdTech investor, 2014

INTRODUCTION

1. Defendant Instructure, Inc. ("Instructure") has built a multibillion-dollar corporate empire by monetizing troves of personal information from users of its products—including millions of school-aged children—without effective consent.

2. Instructure markets itself as an education technology company, but its core business is generating, extracting, and analyzing as much information as possible about students and monetizing that information. The products it markets for use by children in K-12 education are no exception. Through an ever-growing suite of digital products, Instructure generates and extracts personal and private information from school-aged children. It then provides that information to its customers, including schools and school districts, but also more than a thousand private companies. Instructure and its customers convert that information into intimately detailed profiles on children, which they use to develop and market products and services, to manipulate how children think and act, shape their information environment, and make significant decisions affecting their lives and their futures, all without students or their parents ever knowing.

3. Instructure's massive data-harvesting apparatus exposes children to serious and irreversible risks to their privacy, property, and autonomy, and harms them

in ways that are both concealed and profound.

4. Neither students nor their parents[1] 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.

5. None of those elements are met here.

6. Any purported agreement between Instructure and students is not informed: Instructure does not disclose to students, parents, or schools what information it collects and what it does with that information in a reasonably understandable manner.

7. Any purported agreement is not voluntary: because children are required to attend school, they and their parents are coerced into submitting to Instructure's practices.

8. Any purported agreement lacks sufficient consideration: because children are already entitled to education services, Instructure provides them no additional benefit that would support any purported agreement.

9. Any purported consent was not provided by a person with authority to do so. Because most users of Instructure's K-12 products are minors, Instructure is required to obtain their parents' consent before it may take and use their personal and private information. However, Instructure does not seek parental consent before taking and using the personal information of children under 13 through its K-12-marketed products. Instead, Instructure 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 students, any such consent is ineffective. For children 13 and older, Instructure unilaterally purports to shift the burden to schools to obtain parental consent without confirming that such

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

consent was ever obtained.

10. Schools have always collected certain personal information belonging to students and their parents in order to provide educational services, and they must be able to continue to do so—within the bounds of the law. Until recently, that collection was limited and transparent; parents generally knew what information was collected, by whom, and for what purpose, and they could decide if a school crossed a line based on their family's values. But times, and technology, have changed.

11. 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 in not used exclusively for educational purposes; it is used by countless entities for commercial purposes. And the extractive corporate business model does not prioritize positive student outcomes; it prizes "measurability," "scalability," and other profit 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 empty promises of improving education.

12. Instructure acknowledges that "data privacy is a fundamental right[.]" It may not require that children entirely forgo that right in order 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 and how it may be used. Instructure must be held to account for operating as though the fundamental rights of children and their parents are irrelevant.

13. Jasmine Hernandez-Silva and Michael Silva, on behalf of their minor

children M.C. 1[2] and M.C. 2, and Heidi Saas, on behalf of her minor child, M.C. 3, as well as on behalf of all other similarly situated individuals ("Plaintiffs"), by and through their attorneys, bring this class action complaint for injunctive and monetary relief under Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) against Instructure and make the following allegations based upon knowledge as to themselves and the acts of themselves and their minor children, and upon information and belief as to all other matters, as follows:

JURISDICTION AND VENUE

14. This Court has original jurisdiction over the action under the Class Action Fairness Act ("CAFA") of 2005. Pursuant to 28 U.S.C. §§ 1332(d)(2) and (6), this Court has original jurisdiction because the aggregate claims of the putative Class members exceed $5 million, exclusive of interests and costs, and at least one member of the proposed Class is a citizen of a different state than Defendant Instructure.

15. Venue is proper in this District under 28 U.S.C. § 1391 because Instructure is subject to personal jurisdiction here, regularly conducts business in this District, and because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

16. Further, the unlawful conduct alleged in this Class Action Complaint occurred in, was directed to and/or emanated in part from this District. Instructure has sufficient minimum contacts with this state and sufficiently avails itself of the markets of this state through its promotion, sales, licensing, activities, and marketing within this state. Instructure purposely availed itself of the laws of California and engaged and is engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, including persons Instructure knew or had reason to know are located in California, including in

[2] The minor children's names have been anonymized, and they will be referred to herein as Minor Child ("M.C.") 1, 2, and 3.

this District.

THE PARTIES

17. Plaintiff M.C. 1 is a minor. At all relevant times, he has been a citizen of the state of California. M.C. 1 attends school in a California public school district. As part of his public schooling, he was required to access and use Instructure products and services, which he has accessed and used from his school-issued device.

18. Plaintiff M.C. 2 is a minor. At all relevant times, she has been a citizen of the state of California. M.C. 2 attends school in a California public school district. As part of her public schooling, she was required to access and use Instructure products and services, which she has accessed and used from her school-issued device.

19. Plaintiff Jasmine Hernandez-Silva is the mother and legal guardian of Plaintiffs M.C. 1 and M.C. 2. At all relevant times, she has been a citizen of the state of California.

20. Plaintiff Michael Silva is the father and legal guardian of Plaintiffs M.C. 1 and M.C. 2. At all relevant times, he has been a citizen of the state of California.

21. Plaintiff M.C. 3 is a minor. At all relevant times, he has been a citizen of the state of Maryland. M.C. 3 attends school in a Maryland public school district. As part of his public schooling, he was required to access and use Instructure products and services, which he has accessed and used from his school-issued device.

22. Plaintiff Heidi Saas is the mother and legal guardian of Plaintiff M.C. 3. At all relevant times, she has been a citizen of the state of Maryland.

23. Defendant Instructure is a Utah corporation. Its headquarters are located at 6330 South 3000 East, Suite 700, Salt Lake City, Utah 84121.

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.

24. 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."[3] At the heart of that model is an "extraction imperative" that prioritizes maximal collection and monetization of user data.

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

a. generate and collect as much data as possible about a user though the user's 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 sells to 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.

26. 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

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

predictions about them, manipulate their behavior, and influence decision-making about them.

27. Given the extractive and exploitative nature of the surveillance business model,[4] 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.

28. The practices of surveillance capitalism have become commonplace—not just in technological 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 K-12 education.

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

29. The surveillance business model also underpins digital-technology products used in K-12 schools across the U.S.

30. 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 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.

31. By collecting and monetizing children's information, education

[4] The terms "surveillance business model" and "data-monetization business model" are used interchangeably.

technology, or "EdTech,"[5] has become a $250 billion global industry that is projected to nearly triple by 2027.[6]

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

33. Rather than describing a defining feature of any digital-technology 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.

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

35. 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 return."[9]

36. The result is that EdTech has overtaken K-12 education. School districts

---

[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." *EdTech Inc.: Selling, Automating and Globalizing Higher Education in the Digital Age*, Tanner Mirrlees and Shahid Alvi (2019).

[6] 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.

[7] Alex Yelenevych, *The Future of EdTech*, Forbes (December 26, 2022), https://www.forbes.com/sites/forbesbusinesscouncil/2022/12/26/the-future-of-edtech/?sh=7c2924676c2f.

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

[9] *Id*.

access an average of nearly 3,000 EdTech tools during a schoolyear. A single student accesses nearly fifty EdTech tools per year. As Instructure puts it, "[w]hen thinking about the sheer number of technology tools used by a school today, it can be overwhelming."

II. Instructure profits enormously from the personal information of millions of school-aged children.

37. Instructure 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.

38. Schools and school districts pay for Instructure's services with government funds.

39. Instructure does not provide products that merely serve as a kind of digital filing cabinet in which K-12 schools may store education records.

40. Rather, Instructure is an EdTech company specializing in data generation, collection, storage, and analytics.

41. Instructure first became a publicly traded corporation in 2015, was taken private in 2020, and went public again in 2021 at a $2.5 billion valuation. In November 2024, Instructure was again taken private in an all-cash transaction valued at approximately $4.8 billion. Thus, true to its surveillance-capitalist imperative, Instructure has indeed created a return for its investors, which it has done through development and expansion of a far-reaching data-harvesting scheme.

42. Data generation, extraction, collection, analysis, and sharing form the foundation of Instructure's business model.

43. In fact, Instructure has obtained more student data than nearly any other EdTech company. Accordingly, its former CEO Dan Goldsmith once touted, "We have the most comprehensive database on the educational experience in the globe. So given that information that we have, no one else has those data assets at their fingertips to be

able to develop those algorithms and predictive models."

A. Instructure has amassed vast troves of student data.

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

45. Instructure obtains student personal information through its own K-12-marketed products, corporate acquisitions, and third-party data-sharing agreements.

1. Instructure generates and collects student data through its own products.

46. Instructure's primary customers are schools and school districts.

47. By persuading those customers to implement its products in schools, Instructure gains virtually unfettered access to the data of the children who attend those schools, including their personal and private information.

48. By way of just one example, according to its own market research, Instructure's learning management system ("LMS") Canvas is one of the most used LMS systems in the U.S., second only to Google's LMS.

49. Instructure provides its customers access to "massive amounts of data" for the purpose of "assessments, personalization, benchmarking, and engagement."

50. However, Instructure does not publicly disclose the full extent of what data—or even categories of data—it generates and collects from school-aged children.

51. Instructure refuses to make the data it generates and collects from children—or the predictions it generates using that data—available to children or their parents for review.

52. At minimum, Instructure states that it collects the following information from and about students:

a. Student Account Information

i. Basic Identifiers: Name, date of birth, gender/pronouns, email address

ii. Other Identifiers: Profile picture, bio, phone number, home address

iii. Login Credentials: Username, password, avatar

iv. Geographic Information: User location

v. Institutional Information: Academic institution, student ID, Turnitin ID

vi. Third-Party Login Information: Data imported from platforms used for registration/login

vii. Other sensitive personal information: Payments information, parents' names, "Personally Identifiable Information or (PII)," as defined in 34 C.F.R. § 99.3 (FERPA); metadata that is not de-identified

b. Student Activity Data

i. User-Generated Content: Messages, discussion comments, uploaded files (research papers, assignments)

ii. Educational Records: Test results, grades, evaluations, disabilities, socioeconomic information; data types described in the Ed-Fi Data Standard at www.ed-fi.org

iii. Interaction Data: Search activity, time spent on features, date and time of visits

iv. User-Submitted Content: Essays, research reports, portfolios, creative writing, media (music, photos, videos, voice recordings), other uploaded files

v. Career Information: Professional achievements, resume, job descriptions

vi. User Interactions: Messages, comments, uploaded files between users

vii. User-Added Information: Descriptions, images, hashtags associated with uploaded content

c. Device and Usage Data

i. Child User Data: IP address, device identifier, device type, app usage information, persistent identifiers

ii. Device Information: Unique device identifiers, browser type and settings, operating system

iii. Location Information: IP address, geolocation information

iv. Usage Data: Links users have clicked, webpages viewed, time spent on pages and features, referring URLs, language information, how students use Instructure products, students' activities within Instructure products

v. Third-Party Data: Data collected by platforms students access through Instructure products

53. The data Instructure generates and extracts from students far exceeds what could be legally or traditionally characterized as "education records."

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

55. The data Instructure obtains, when combined with other data and processed, enables Instructure and its many third-party partners to build dynamic, robust, and intimate dossiers of children.

56. The amount of data Instructure collects about children, including children under 13, far exceeds that which is reasonably necessary for children to participate in any school activity that is facilitated by Instructure products and services in violation of the Children's Online Privacy Protection Act ("COPPA"). *See* 15 U.S.C. § 6502; 16 C.F.R. § 312.7.

57. Instructure could design the products it markets and sells to K-12 education institutions to minimize the amount of data it collects from students. Instead, Instructure optimizes its products for data extraction, including those products marketed by use for children in compulsory education environments.

58. That Instructure's K-12-marketed products are not designed to optimize for student privacy is an intentional, self-interested choice that comes at the expense of children's privacy, safety, and autonomy.

2. Instructure obtains student data through corporate acquisitions.

59. In addition to obtaining student data when students use its products, Instructure also obtains student data through corporate acquisitions. Indeed, student data is a valuable asset of an acquisition target.

60. Since 2015, Instructure has acquired nearly a dozen companies, which it has fully integrated into its student data and data-derivative ecosystem.

61. Some of these acquisitions include the 2024 purchase of Scribbles Software, a student data and workflow management platform; the 2023 purchase of Parchment, a digital-credentials and academic-records management platform; the 2022 purchase of LearnPlatform, an EdTech efficacy-assessment platform; the 2022 purchase of Concentric Sky, a platform that catalogs students' academic performance and skill development; the 2021 purchase of Kimono, a platform that facilitates data syncing across EdTech applications; the 2019 purchase of MasteryConnect, an assessment and curriculum platform; and the 2019 purchase of Portfolium, a career-readiness platform.

62. Instructure's data trove now includes data from the many platforms it has acquired, such as comprehensive student data from Scribbles; academic records and associated personal information from Parchment; EdTech usage data from LearnPlatform; algorithmic predictions and inferences from MasteryConnect; and detailed student career portfolio information from Portfolium.

63. These acquisitions—and the student data Instructure gains as a result—are essential to Instructure's data-monetization business model.

3. Instructure obtains user data through data-sharing agreements.

64. In addition to collecting personal information from children through its own products and corporate acquisitions, Instructure also obtains such data through

data-sharing agreements with more than one thousand companies.

65. Instructure has robust data-sharing agreements through which third-party partners provide Instructure data to support the development, maintenance, improvement, and marketing of Instructure's products.

66. Instructure partners with more than one thousand third-party companies with which it exchanges user data.

67. Under the guise of "interoperability," Instructure has intentionally architected its data-sharing ecosystem to maximally ingest data from partner companies, including, but not limited to, school information system ("SIS") platforms.

B. Instructure uses and discloses users' personal information for a variety of commercial and other purposes.

68. Instructure uses and discloses the personal information it generates, extracts, and collects from children and their parents for a host of purposes, including commercial purposes that exceed legitimate educational purposes.

69. By its own terms, Instructure uses and discloses students' information in at least the following ways:

a. Create and maintain user accounts;

b. Identify users;

c. Provide, administer, maintain, and improve its products;

d. Support internal operations;

e. Personalize the user experience;

f. Provide technical and other customer support;

g. Contact and communicate with users;

h. Solicit feedback about its products, including asking users to respond to surveys or questionnaires;

i. Analyze trends;

j. Track users' movements around products;

k. Share with third-party service providers;

l. Disclose to any other third party at a school's direction;

m. Transfer as part of a merger or acquisition;

n. Disclose as part of a bankruptcy proceeding;

o. Comply with court orders and other legal processes;

p. When Instructure believes it is necessary to prevent violation of its terms of service or other policies;

q. When Instructure believes it is necessary to take action regarding litigation in which Instructure is involved; and

r. So-called "de-identified or aggregate information" for any purpose.

70. The following elaborates upon just a few of these uses and disclosures.

1. Instructure uses children's data to develop digital products for, and market those products to, current and potential customers.

71. Like most surveillance-technology companies, Instructure does not collect user data for the primary purpose of providing the raw data itself to third parties nor for the limited purpose of assisting students with their educational pursuits. Instead, it collects, combines, and analyzes children's data for the purpose of building highly detailed and intimately personal dossiers of them, including their preferences, behaviors, and aptitudes, which they use to generate myriad purported predictions about a child's life.[10]

72. Instructure sells predictions concerning a wide range of a child's attributes

[10] Alyson Klein, *Education Week*, "Most Tech Companies Profit Off Student Data, Even If They Say Otherwise, Report Finds," (July 18, 2023), https://www.edweek.org/technology/most-tech-companies-profit-off-student-data-even-if-they-say-otherwise-report-finds/2023/07?eType=EmailBlastContent&eId=7efdbba7-9fcf-40d8-8c96-2c628bde1f1c.

and behaviors, such as her future academic performance, skill mastery, learning comprehension, interests, risks, behavior, college and job readiness, and more. These predictions are variously described as "insights," "analytics," "diagnostics," "assessments," "products," "offerings," "solutions," "guidance," and other such intentionally esoteric, anodyne terms.[11]

73. Instructure's third-party customers use those products to identify, target, manipulate, make decisions about, and otherwise control or monetize children and their personal information. For Instructure's school customers, such purposes include, without limitation, automating learning evaluation methods (such as aptitude), comprehension testing, development of "personalized" curricula or "learning journeys," student management and oversight, and other aspects of school administration and education, all under the guise of improving education.

74. Although Instructure markets these products as conferring administrative and pedagogical benefits to schools and school districts, they are undeniably commercial, for-profit products that have enabled Instructure to build a multibillion-dollar surveillance-technology empire at the expense of student privacy.

75. Instructure's products are designed to work synergistically to collect data on every aspect of an individual's persona and then manipulate that data to influence the student and their parents. The data is then marketed to Instructure's current and prospective third-party customers in service of Instructure's bottom line.

76. Data flows freely between products in support of what Instructure calls its "Instructure Ed-cosystem."

77. Fueled by its ever-growing trove of student data, Instructure's suite of products now includes dozens of data-derived products, not limited to the following:

a. **Canvas LMS** – a centralized platform for managing and delivering online

[11] *See*, *e.g.*, Cathy O'Neil, *Weapons of Math Destruction*, (2016); Zuboff, *The Age of Surveillance Capitalism*.

learning experiences.

b. **Canvas Studio** – an interactive video platform and engagement analytics.

c. **Canvas Catalog** – a district-branded digital course catalog and registration system.

d. **Canvas Credentials** – a digital-badging platform that creates a portable "comprehensive learner record" of student progress.

e. **Canvas Student Pathways** – platforms that create a personalized "learning journey" for students "up to graduation and beyond." Provides children with a "lifelong digital portfolio" comprised of "badges, pathways, coursework, and portfolios with peers, mentors, and potential employers."

f. **Canvas Student ePortfolio** – allows employers to search and select job candidates from student databases.

g. **Mastery Connect** – digital personalized assessment platform that lets teachers monitor and track student progress (on Instructure-created assessments). Uses traditional scoring. Provides "instant insights" on student progress and identifies areas for intervention. Fully integrates with Canvas.

h. **Mastery Item Bank** – a collection of assessment questions teachers can use to create assessments for use in Mastery Connect. Provides teachers "immediate feedback" and "meaningful insights" (included with Mastery Connect).

i. **Mastery View Formative Assessments** – a compilation of complete, pre-built instructional assessments for use in mastery connect. Uses Diagnostic Classification Model scoring to provide diagnostic insights and create personalized learning plans (available at an additional cost).

j. **Mastery View Predictive Assessments** – pre-built benchmark assessments designed to enable schools to predict how students will perform on standardized tests.

k. **Mastery View College Prep Assessments** – ACT preparatory tests.

l. **Elevate Data Quality** – programmatically assesses all district data for quality to support decision-making and fundraising.

m. **Impact** – assesses the efficacy of EdTech products to "drive adoption of new technology tools." Monitors students' engagement with all such platforms and provide "a bird's-eye view of how deeply students . . . are engaging with tech tools" by providing student usage analytics.

n. **Intelligent Insights** – "leverages AI and analytics to enable data-informed decisions" for decision-making purposes, for example, understanding how kids use EdTech, identifying "at-risk learners," or assessing course readiness, by providing "real-time monitoring" of students.

o. **LearnPlatform EdTech Effectiveness** – provides third-party edtech providers with "evidence" based on "research" conducted by Instructure staff to drive marketing and sales ("evidence-as-a-service").

p. **Elevate Standards Alignment** – another tool marketed to third-party edtech providers to help market and sell their products and services by improving compliance with relevant standards.

q. **Elevate Data Sync** – interoperability tool that facilitates flow and synchronicity of data between systems and platforms (e.g., SIS and LMS).

r. **Elevate Data Sync for Partners** – transfers data from schools to third-party vendors. "Make it easy for [schools] to share [student] data with your application. Data Sync continuously exchanges data between SIS and your application," such as Google's K-12 products.

78. Instructure also uses the information to develop its artificial intelligence ("AI") technologies, which Instructure is actively incorporating into its suite of K-12 products.

79. To power its massive and growing suite of data-derivative products and provide its customers access to granular student analytics, Instructure compiles the data it collects through each of its platforms and uses it to build, improve, and market its suite of products to third parties.

80. Student data generated and extracted through Instructure's platforms is not segregated, and the collection and use of that data is not limited to only the products licensed by schools. Rather, Instructure consolidates all of the data it collects from

schools and directly from students to enhance its suite of products to facilitate deeper and more individualized analytics, which are marketed to third parties as enabling greater targeting of, and decision-making about, students.

81. This aggregation and sharing of student data is core to Instructure's data-monetization business model.

2. Instructure obtains and discloses student data through third-party data-sharing agreements with more than 1,000 companies.

82. Instructure partners with *more than a thousand companies* in the generation, collecting, analysis, use, and sharing of student data.

83. These partners include integration partners, service partners, and sales and marketing partners, such as:

a. **TurboVote** – voter registration and "preregistration" for minors.

b. **Panopto** – providing AI video tools.

c. **Illumidesk** – using AI to provide customers "[a]ny data source, any insight, at everyone's fingertips."

d. **ScreenPal** (formerly Screencast-O-Matic) – specializing in AI-assisted screen and webcam recording.

e. **Echo360** – monitors, tracks, and increases student engagement with its own and third-party platforms and products in the "Edcosystem"—an "interoperable, modular end-to-end suite of solutions—providing customers granular data on student online activity and habits, "making it simple to track each student's progress in the moment and long-term." Serves education, corporate, and government customers.

f. **Iseek.ai** – "Your AI Platform for Data Discovery" supporting "better decision-making with groundbreaking search and analytics solutions."

g. **Mercer Mettl** – a global online talent assessment platform that helps customers make hiring decisions.

84. Instructure states that "[w]e've worked to build a robust partner

community where we work together with trusted education partners to deliver all things awesome," with a focus on product and data integration.

85. Instructure markets to prospective partners that they can "[b]enefit from a supportive partnership program to maximize profits in education" and gain "comprehensive enablement for your teams to capitalize on EdTech's rapid expansion."

86. Its primary value to third-party partners depends on maximizing access to student data.

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

88. Instructure markets to prospective partners that partnership will "[g]row your reach and your impact with exclusive Instructure partner benefits, tools, and opportunities," and "[i]ntensify your educational impact with tools to build, scale, and continuously improve; access to Instructure's community of 30+ million users; and unique opportunities to connect directly with the Instructure team."

89. Instructure touts that it designs its products to "deliver an open, extensible learning ecosystem," with an "[e]mphasis on OPEN." It notes that "Canvas is a total open platform – open in everything from an OPEN API that allows for customer integrations, to OPEN DATA . . . ." It describes its partnership ecosystem as "a community that centers itself around low-cost plug and play integrations."

90. Instructure shares student data in real time and/or near-real time.

91. Instructure does not meaningfully limit the amount of student data that partners can access. The only limit it imposes is "throttling," which limits the amount of data that may requested at a given time on an as-needed, technical basis.

92. Instructure requires that students enable third-party cookies at the browser

level in order to use Canvas, which unnecessarily exposes the user device and data to serious and ongoing security risks.

93. The "Instructure Ed-cosystem" is "built on an open API" that works "with 500+ like-minded partners" to develop products and services.

94. The Instructure Representational State Transfer Application Programming Interface ("REST API" or "API") is how third parties interact programmatically with Instructure products. It allows third-party developers to build integrations and provides robust access to vast troves of personal information of "Data Subjects"—including school-aged children—through Instructure's suite of products.

95. The API provides third-party partners programmatic access to Canvas user data for a host of commercial purposes, including data harvesting, analysis, disclosure, and training AI systems. Indeed, Instructure retains a commission of 30 percent of the net revenues generated through the sale of any partner AI product to an Instructure customer.

96. Instructure touts to shareholders that its "partnership program invites third-party software, service and content providers, through a library of open APIs, to easily integrate with our applications and take advantage of value add services and events to enhance the partnership." In the context of the Instructure API, an "event" refers to a specific action or occurrence within the Canvas platform that triggers a data notification or update. In other words, Instructure gives third parties broad access to all manner of data generated about and extracted from children anytime those children interact with the Canvas ecosystem.

97. Instructure "Live Events" are "specific events emitted by Canvas when an interesting action takes place, such as a page being accessed, a student submitting an assignment, or course settings being updated." Live Events "captures detailed events when a user traverses a Canvas account or course" and provides partners access to granular, child-specific information, such as time taken to finish a test, when a student

submits a test, how long a child uses a product at a time, "common patterns" among a child's product usage, what assignments are most challenging.

98. According to Instructure, its partners desiring "the most up-to-date information possible [] should use the regular Canvas API instead of Live Events." With Canvas API, a data event is relayed upon essentially any activity within Canvas products. It grants third parties access to detailed user data relating to dozens of "triggering events", including, but not limited to:

a. Account creation and use
b. Assignments
c. Addition of files
d. Addition or creation of content
e. User communications and group discussions
f. Individual grades and outcomes
g. Group grades and outcomes
h. Login activity
i. Outcome calculation methods
j. Quiz submissions
k. Rubric assessments
l. Student Information System imports
m. Assignment or assessment submission details
n. Syllabus
o. User information
p. Asset (which appears to be a sort of catchall category of data events)

99. Instructure provides partners extensive data "Payload Examples" for each triggering event, or the data transmitted through the system upon the occurrence of such event.

100. For example, when a student is added to a Canvas account, partners have access to the student's identifying information:

Field	Description
created_at	The time at which this user was created.
name	Name of user.
short_name	Short name of user.
updated_at	The time at which this user was last modified in any way.
user_id	The Canvas id of user.
user_login	The login of the current user.
user_sis_id	The SIS id of the user.
uuid	Unique user id.
workflow_state	State of the user.

101. When a student submits assignments, partners can access various data, such as the student's "Canvas ID," content and grade of a student's submissions, when an assignment was submitted, and whether the assignment was submitted late:

Field	Description
assignment_id	The Canvas id of the assignment being submitted.
attempt	This is the submission attempt number.
body	The content of the submission, if it was submitted directly in a text field. NOTE: This field will be truncated to only include the first 8192 character
grade	The grade for the submission, translated into the assignment grading scheme (so a letter grade, for example)
graded_at	The timestamp when the assignment was graded, if it was graded.
group_id	The submissions's group ID if the assignment is a group assignment.
late	Whether the submission was made after the applicable due date.
lti_assignment_id	The LTI assignment guid of the submission's assignment
lti_user_id	The Lti id of the user associated with the submission.
missing	Whether the submission is missing, which generally means past-due and not yet submitted.
score	The raw score
submission_id	The Canvas id of the new submission.
submission_type	The types of submission (basic_lti_launch, discussion_topic, media_recording, online_quiz, online_text_entry, online_upload, online_url)
submitted_at	The timestamp when the assignment was submitted.
workflow_state	The state of the submission: normally 'submitted' or 'pending_review'.
updated_at	The time at which this assignment was last modified in any way
url	The URL of the submission (for 'online_url' submissions)
user_id	The Canvas id of the user associated with the submission.

102. Once a student's assignment is graded, partners can access that data, too, such as the student's Canvas ID, when her assignment was graded, what the grade was, the student's grade in the class, and even unsubmitted assignments:

Field	Description
user_id	The Canvas user ID of the student.
course_id	The Canvas ID of the course.
workflow_state	The state of the score record in the database, could be "active" or "deleted".
created_at	The time when the row in the scores table (representing the course grade) was created. The score row is created as a result of some grade calculation, even if there are not yet any graded submissions for a student, i.e. when a student is enrolled in the class.
updated_at	The time when the row in the scores table was last updated -- that is, when the event is emitted.
current_score	The user's current score in the class.
old_current_score	The user's current score in the class before it was changed. This field will not be available until a student submits the first assignment in the class.
final_score	The user's final score for the class.
old_final_score	The user's final score for the class before it was changed. This field will be set to 0.0 until a student submits the first assignment in the class.
unposted_current_score	The user's current grade in the class including unposted assignments.
old_unposted_current_score	The user's current grade in the class including unposted assignments, before it was changed. This field will not be available until a student submits the first assignment in the class.
unposted_final_score	The user's final grade for the class including unposted assignments.
old_unposted_final_score	The user's final grade for the class including unposted assignments, before it was changed. This field will not be available when a student submits the first assignment in the class.

103. Third parties may also access information about a student's location; how and how long the student interacts with "assets" within the Instructure ecosystem, including Instructure and third-party products; the student's learning progress, including whether a student achieved mastery of a learning outcome and how many attempts it took student to master an outcome; and a host of other sensitive and personal information about students.

104. Instructure states that personal data that is processed and/or transferred to partners includes demographic data, technical data, metadata, or any other personal data processed by the partner service.

105. Instructure states that the frequency and duration of the transfer of such data is "continuous for the term of the Agreement."

106. Instructure permits partners to include children's personal information in

their products as necessary for the partner to provide its product.

107. Instructure prohibits partners from responding to requests from "Data Subjects" regarding their personal information and other "Data Subject rights" without Instructure's prior written consent. Instructure thus contractually prohibits third parties from complying with their obligations under COPPA.

108. Instructure prohibits partners from returning or deleting personal data except "at Instructure's sole discretion, within 90 days after termination of the [data-sharing] Agreement, or within 30 days upon receipt of written request by Instructure." Instructure thus contractually prohibits third parties from complying with their obligations under COPPA.

109. The result is that, through its suite of K-12-marketed products, Instructure and innumerable third parties generate and gain access to an enormous volume of data from and about students and their families, while preventing them from even accessing their own information.

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

110. Instructure fails to obtain effective consent for its sweeping collection and use of user data, including students' personal and private information. Specifically, Instructure fails to (1) provide sufficient 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 sufficient consideration in exchange for their valuable personal and private information.

A. Instructure fails to provide sufficient information to support informed consent.

1. Instructure fails to provide reasonably understandable information about its data practices.

111. For consent to be effective, Instructure's disclosures must explicitly notify

users of the specific conduct and practices at issue.

112. Instructure is required to provide disclosures regarding its data practices that a reasonable person would understand and know what they were consenting to.

113. Further, before collecting personal information from children under 13, Instructure is required to provide parents 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.

114. A reasonable user cannot understand Instructure's data practices by reviewing Instructure's disclosures.

115. Instructure itself has observed a "[l]ack of transparency for users" and noted that, "[w]ithout a trained privacy or IT expert, it can be difficult to ensure the terms of service align with district policies." Such terms are legally inadequate.

116. Instructure fails to provide children and their parents information that they may reasonably understand that 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.

117. Instructure also fails to provide parents of students under 13 notice of its data practices that is clearly and understandably written, complete, and contains no unrelated, confusing, or contradictory materials.

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

a. Master Terms and Conditions

b. Terms of Use

c. Product Privacy Notice

d. Instructure COPPA Privacy Policy

e. Data Processing Addendum Policy

f. Master Service Agreement Policy

g. Acceptable Use Policy

h. SDPC Resource Registry (to locate Instructure's Student Data Privacy Agreements with Local Education Agencies)

i. Ed-Fi Data Standard

j. Google API Services User Data Policy

k. Google Privacy Policy

l. YouTube Terms of Service

m. Instructure Partners

n. Partner Program Terms and Conditions and Addenda

o. Marketing Privacy Policy

p. California Privacy Notice Policy

q. Canvas Badges Terms of Service

r. Canvas Badges Business Account Privacy Policy

s. Canvas Badges Data Processing Addendum

119. Instructure's various terms and policies also reference other materials that are not readily available to users. For example, its Product Privacy Notice states that a student's school will have a privacy notice that governs use of their personal information. The Master Terms and Conditions refer to a separate Agreement between customers (defined only as the entity identified in the Agreement) and Instructure. The Data Process Addendum also refers to a separate Agreement between "Customers" and Instructure. The Partner Program Terms similarly refer to a separate Agreement

between partners and Instructure that take priority over those Terms.

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

121. Indeed, it is impossible for any reasonable person to fully understand the extent of Instructure's and its partners' generation, collection, aggregation, use, and sharing of personal information about and belonging to school-aged children.

122. Instructure's disclosures thus fail to meet generally applicable data-privacy standards, as well as the heightened notice requirements of COPPA, which provide additional protections to children under 13. *See* 15 U.S.C. § 6502; 16 C.F.R. § 312.4.

2. Instructure does not and will not disclose the full data set it has collected on individual students or parents.

123. In addition to providing wholly deficient disclosures, Instructure fails to provide parents access to, control over, or information about the data it collects from them or their children—including children under 13—and the information associated with or generated using that data, as would be necessary to (1) ensure Instructure's compliance with its own terms of service and privacy policies, (2) support ongoing effective consent, and (3) comply with COPPA.

124. Instructure's COPPA policy states that parents have a right to review, correct, and delete their children's information and to demand that Instructure cease collecting their information.

125. However, when Plaintiff Saas requested access to her child's personal information, Instructure did not provide her access to her child's data.

126. On information and belief, Instructure has a policy of denying parents access to their children's data.

127. When Plaintiff Saas attempted to access that information through her school district, her district provided certain limited records and noted that other requested records "do not exist at [the school] but may exist with Instructure[.]"

128. Students and parents thus have no way to control—correct, delete, or otherwise modify—or even review students' personal and private information that is generated, taken, and used by Instructure.

129. Students and parents do not and cannot know the full extent of the data Instructure obtains about them, whether that data is accurate, how that data is stored, how long that data is retained, who has access to that data, or how that data or data-derivative information or products are used.

130. Plaintiffs do not have a reasonable understanding of Instructure's data practices as a result of Instructure's failure to adequately disclose its practices.

131. Without any such access, control, or information, effective, ongoing consent to Instructure's data practices is not possible.

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

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

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

134. 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.

135. Because minors are not legally competent to provide valid, binding consent, the collection of data from children requires parental consent.

136. Further, COPPA contains a heightened parental-consent requirement that Instructure must meet before it may collect personal information from children under 13. *See* 16 C.F.R. § 312.5. Specifically, COPPA requires that Instructure "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). Instructure has not done so and does not meet any of the exceptions to COPPA's consent requirement. *Id*. § 312.5(c).

137. Instructure at no time obtains effective consent from children or their parents for its collection or use of their data as described herein, under generally applicable standards or the heightened COPPA standards.

138. Instead, for children 13 and older, Instructure purports to unilaterally shift the burden to schools to obtain the necessary consent for Instructure's creation, collection, and use of student data without obtaining any manifestation of assent by students or parents themselves. Instructure's Master Terms and Conditions state that school customers agree to "obtain from Users any consents necessary under this Agreement or to allow Instructure to provide the service[.]"

139. For children under 13, Instructure relies on the school's consent *alone*. Its COPPA Privacy Policy states that "the School provides consent to this collection and use of personal information from and about Children as required under applicable laws, including COPPA."

140. Thus, for children 13 and older, Instructure purportedly shifts the burden to schools to obtain parental consent. But for children under 13, counterintuitively, Instructure does not even seek parental consent before taking their information, leaving parents of young children with fewer rights—and their children less protected—than older students.

141. Schools do not own the personal and private information that Instructure

generates about students or extracts directly from students.

142. School administrators are not legal guardians of students.

143. Students own their own personal and private information.

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

145. Schools do not control the generation, collection, storage, use, or disclosure of student data by Instructure or any third party to which Instructure grants access to student data.

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

147. Instructure generates and obtains student data in excess of education records.

148. Instructure generates, obtains, and uses student data in excess of legitimate educational interests.

149. Instructure rediscloses children's personal information to a host of third parties without obtaining prior parental consent.

150. Plaintiffs did not consent to Instructure's taking and using their children's information.

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

152. Instructure thus collects, uses, and discloses children's personal information without obtaining effective consent.

C. Students' use of Instructure's products is not voluntary as would be necessary to support their agreement to Instructure's data practices.

153. Voluntariness is an essential element of contract formation.

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

155. Every state in the United States has compulsory education laws.

156. Schools use Instructure's products to support a host of pedagogical and administrative functions.

157. Plaintiffs were not given a choice to forgo using Instructure's products at their school.

158. Even if students theoretically could opt out of using Instructure's products, Instructure may not place students and their parents in the position of having to choose between their rights 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.

159. Because students and parents lack the ability to decline or avoid use of Instructure's products, any purported agreement by them to Instructure's terms and policies is unenforceable.

D. Instructure does not provide students sufficient consideration as necessary to support any agreement to Instructure's data practices.

160. Consideration, or the legal exchange by parties of something of value, is an essential element of contract formation.

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

162. Every state in the United States, including California, has laws guaranteeing children the right to an education.

163. That right includes the right for students to avail themselves of

educational services offered by their school.

164. Schools use Instructure's products to support a host of pedagogical and administrative functions.

165. Children are also legally obligated to attend school.

166. Students' use of Instructure's products is thus a part of the education to which they are already legally entitled.

167. Instructure 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 Instructure's terms and policies, including those governing Instructure's data practices.

168. Plaintiffs were provided no additional consideration that might have supported any purported agreement to Instructure's data practices.

169. Any purported agreement between Instructure and students is not supported by the exchange of any new benefit to students.

170. Without consideration, Instructure may not show the existence of an agreement between itself and the students whose information it takes and uses.

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

171. Instructure makes false and misleading statements regarding its data practices on which it intends the public, school personnel, and parents to rely.

172. Instructure falsely touts its commitment to privacy, including at the top of its privacy page:

173. In an article entitled "Our 5 Guiding Principles" written by Instructure's Associate General Counsel and Data Protection Officer published on Instructure's website, Instructure falsely states that "privacy standards are embedded in our corporate DNA" and that its approach to privacy is "built upon five key principles: transparency, accountability, integrity, security, and confidentiality."

174. In an article entitled "Our Foundation of Privacy" written by Instructure's Chief People and Legal Officer published on Instructure's website, Instructure falsely states that it "takes its responsibility of protecting your data seriously."

175. Instructure does not take data privacy seriously. Instructure instead takes seriously the duties it owes to its shareholders, whom it warns about the challenges that privacy laws and expectations can pose to Instructure's business model as detailed in an annual shareholder report. Indeed, Instructure warns shareholders that the possibility of lawsuits related to its data practices could require it "to fundamentally change our business activities and practices or modify our learning platform and platform capabilities, which could have an adverse effect on our business."

176. Instructure tells shareholders nothing of data minimization, its purported "Foundation of Privacy," or its internal commitment to privacy and "radical transparency."

177. Instructure's data practices and shareholder disclosures directly undermine its publicly stated privacy principles.

178. In that same "Our Foundation of Privacy" article, Instructure falsely states that its products are "private by design." In fact, its products are designed to maximize the generation, collection, use, and sharing of student data among its own products as well as third-party products.

179. To shareholders, Instructure touts the features of its platforms and data practices, frequently employing terms such as open, highly integrated, accessible, complete, comprehensive, extendable, measurable, connected, and the like. These

concepts are antithetical to privacy. Instructure's products are not designed to optimize for both privacy and openness. Instructure publicly touts the former while privately designing for the latter.

180. On its own privacy and security page on its website, Instructure misleadingly states that it protects information it "receive[s] by ensuring it's used only to support students, institutions, and education." In fact, Instructure not only receives information, it actively generates and extracts information directly from children and their parents, which it and myriad undisclosed third parties use for their own commercial benefit.

181. In its COPPA Privacy Policy, Instructure falsely states that it "will not require a School or Child to disclose more information than is reasonably necessary to use our Services." Instructure obtains far more information than is reasonably necessary to provide children and schools education services, including data obtained to develop and market the products of Instructure and myriad third parties.

182. On the "Institutions and Educators Privacy FAQ" page in the privacy section of its website, Instructure misleadingly states that it does not sell information to third parties, while failing to disclose to decision-makers that it makes information widely available to enumerable third parties under robust data-sharing agreements. Indeed, Instructure advises shareholders that its integration with its partner network "allows us to broaden and efficiently extend the functionality of our applications."

183. In an article entitled, "Power to the People with Canvas Data and Analytics (Can You Dig It?)" published on its website, Instructure falsely states that it does not monetize user data because it uses that data to improve its products instead of using it to "sell[] college branded hoodies," while failing to explain any legal distinction between use of data to develop physical products versus digital products for commercial purposes.

184. In its COPPA Privacy Policy, Instructure falsely states that it does "not use

personal information about Children for our own commercial purposes." But Instructure does use children's personal information for commercial purposes, as described herein.

185. In its COPPA Privacy Policy, Instructure also falsely states that it complies with COPPA. In fact, Instructure violates numerous provisions of COPPA as described herein. For example, with respect to children under 13:

a. Instructure fails to provide complete, understandable notice of its data practices;

b. Instructure fails to obtain parental consent before taking and using children's personal information;

c. Instructure falsely informs schools that they are authorized to consent in lieu of parents under COPPA;

d. Instructure collects more personal information from children than is necessary for children to participate in school activities facilitated by Instructure;

e. Instructure retains children's personal information for longer than is necessary to fulfill the stated purposed for which the information was collected; and

f. Instructure fails to provide parents access to the personal information it has collected from their children.

186. In its Product Privacy Policy, Instructure falsely states that it provides parents the ability to access, review, delete, and otherwise control their children's information.

187. In its Product Privacy Policy, Instructure further 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 use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students."

d. "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."

e. "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."

f. "We will support access to and correction of Student PII by the student or their authorized parent[.]"

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

188. Instructure does not adhere to these commitments, as described herein.

189. Instructure intends that the public—including school personnel and parents—rely on these statements in determining whether and how to use its products.

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

191. 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 Instructure's exploitative data practices, especially while attending school and engaging in school activities, such as completing assignments and

communicating with teachers.

192. As Instructure warns its shareholders: "Our publication of our privacy policy and other statements we publish that provide promises and assurances about privacy and security can subject us to potential state and federal action if they are found to be deceptive or misrepresentative of our practices."

V. Instructure's nonconsensual data practices harm children.

193. Instructure's surreptitious data practices are not benign. Rather, they harm children in myriad ways that are immediate, significant, and long-lasting.

194. Instructure's practices irreparably damage school-aged children by violating their privacy and their right to access and control their own personal and private information.

195. Instructure's practices, as described in this complaint, also harm students in the form of diminution of the value of their private and personally identifiable data and content.

196. The inability to control this data and Instructure's collection and use thereof further impedes students' ability to control what is done with their data after Instructure takes it.

197. Parents are entitled to be fully informed of the potential benefits and risks that Instructure's data practices pose to all education stakeholders, especially children. Once fully informed, it is up to parents 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.

A. Instructure harms children by invading their privacy.

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

199. The right to privacy begins with protection from having information created about a person in the first instance.

200. The right to privacy encompasses the person's right to control information concerning his or her person. Loss of such control harms a person's ability to, for example, manage and minimize risk.

201. As Instructure puts it, "privacy is the right to be left alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used. Here at Instructure, we believe that data privacy is a fundamental right[.]"

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

203. Instructure collects, for its own commercial benefit, data about public-school kids from information that the students share 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 the social norms.

204. Further, Instructure does not provide children and their parents access to or control over children's personal information.

205. 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.

206. 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."[12]

[12] Noah Joshua Phillips, Taking Care: The American Approach to Protecting Children's Privacy, Federal Trade Commission (November 15, 2018), https://www.ftc.gov/system/files/documents/public_statements/1422695/phillips_-_taking_care_11-15-18_0.pdf.

207. The information Instructure collects is used in countless ways that infringe upon the many time-honored privacy rights of children.

208. Instructure's sweeping generation, collection, use, and disclosure of personal and private information about and belonging to children is highly offensive by any standard.

B. Instructure harms children by persistently surveilling them.

209. Instructure harms children by persistently surveilling, monitoring, and tracking them while they use its products.

210. Research has shown that persistent surveillance decreases opportunities for children to exercise autonomy and independence. Persistent surveillance hinders children's development of self-regulation and decision-making that are crucial to aspects of responsibility and self-identity.[13] 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.[14] Continuous surveillance emphasizes compliance with the current social order instead of the cultivation of identity and dignity.[15]

211. Persistent surveillance at school normalizes surveillance in other areas of life and trains children not to value their own and others' privacy and autonomy.[16] It also normalizes the exploitation of children, their personal information, and their educational development for third-party commercial gain without knowledge, consent, or compensation.[17]

---

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

[14] *Id*.

[15] *Id*.

[16] *Id.* at 6.

[17] *Id*. at 7.

212. The oppressive effect of Instructure's surveillance practices is proportional to the invisibility and pervasiveness of those practices.[18]

C. Instructure harms children by compromising the security of their personal information.

213. By collecting and storing children's personal information—and by creating information about them that did not previously exist—Instructure forever jeopardizes children's information by making it vulnerable to a host of data security risks.

214. Rates of cybercrime are steadily rising, including numerous data breaches that affect a host of consumers and their personal information.

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

216. In fact, another leading student information system was hacked in December 2024, compromising the personal information of tens of millions of students.[19]

217. Such exposure 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."[20]

218. Instructure admits that "student data is even more sensitive than general personal data," and that "[s]tudents, especially younger children, are not yet equipped

[18] *Id*. at 3.

[19] TechCrunch, Malware stole internal PowerSchool passwords from engineer's hacked computer, https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-passwords-from-engineers-hacked-computer/

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

to weigh the potential benefits and risks of data loss."

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

220. Children's data is further compromised by Instructure's practice of providing access and otherwise sharing that information with an ever-growing multitude of third parties.

221. In sum, Instructure's data practices harm children from the moment their personal information is generated or otherwise obtained by Instructure. That harm is exacerbated by Instructure's persistent storage, use, and disclosure of that information to its network of over one thousand third parties.

D. Instructure harms children by affecting their access to information and opportunities through algorithmic profiling.

222. As described herein, Instructure uses student data to create products that purport to analyze and predict student performance and behavior.

223. Instructure markets these analytics to its customers for use in wide-ranging decision-making about children, a practice known as algorithmic profiling. Such analytics purport to help teachers and administrators "personalize" a child's curriculum and learning plan, understand a child's strengths and weaknesses, identify a student's individual education goals, formulate plans for reaching those goals, and a host of other predictions and recommendations for purportedly better management of the child.

224. Instructure's algorithms attempt to gather children's knowledge, understanding, and potential to reduce them to quantifiable analytics. In doing so, there is an inherent sacrifice of accuracy, nuance, and privacy for efficiency, measurability, and scalability.

225. These models define their own metrics, which Instructure uses to justify their results, creating and perpetuating a pernicious and untested feedback loop.

226. Some of Instructure's platforms are designed to assist colleges and employers with recruitment by providing them access to data-derived student "insights."

227. By generating these predictions on which myriad third parties rely in making consequential decisions affecting children, Instructure produces and sells the equivalent of credit reports on children in every domain over which Instructure claims algorithmic expertise.

228. The datafication of a child and their learning process, for commercial purposes, brings about a social disempowerment that negatively affects the child's education in the moment of learning and also, therefore, the future of a free and sustainable society.[21]

E. Instructure harms children by denying them access to their data and subjecting them to data practices that are opaque, unreviewable, and unappealable.

229. Beyond taking and using children's personal information for purposes of algorithmic profiling, Instructure denies children and their parents the ability to access and review the data it takes from them and understand how it is used and whom has access to it.

230. Further, the algorithmic models on which Instructure's products are built are opaque.

231. Children and their parents are thus unable to review the data collected and aggregated about them, the algorithmic models used to generate predictions, the

[21] *See, e.g.*, Nottingham, Stockman, Burke, *Education in a datafied world: Balancing children's rights and school's responsibilities in the age of COVID 19*, Computer Law & Security Review (July 2022) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8958095/pdf/main.pdf.

assumptions on which those models are based, or otherwise understand how their data is processed, interpreted, and used.

232. As previously discussed, schools and other third parties may rely on the data collected by Instructure and the data-derived products generated by Instructure to make decisions that affect children's lives now and in the future.

233. Instructure's practices harm children by denying them and their parents the ability to: (1) assert their rights by providing—or declining to provide—consent before their information is taken and irreversibly compromised; (2) respond effectively to issues involving their personal information; or (3) make meaningful decisions regarding the collection, storage, and use of their information. Children are also unable to know and object to the predictions generated by unknown data and how third parties use those predictions.

234. By denying families the ability to review and understand this information—thereby denying them the ability to identify, assess, and seek redress of attendant harms—Instructure's practices are deceptive, unfair, and unconscionable, especially given that Instructure conscripts children into this opaque corporate apparatus without parental notice or consent in the first instance.

F. Instructure harms children by failing to compensate them for their valuable property and labor.

235. Personal data is now viewed as a form of currency in today's data economy. There has long been a growing consensus that consumers' sensitive and valuable personal information would become the new frontier of financial exploitation.

236. A robust market exists for user data, especially children's personal information. That market has been analogized to the "oil" of the digital economy.[22]

[22] The Economist, "The world's most valuable resource is no longer oil, but data" (2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

237. Furthermore, most consumers value their data and their privacy. Accordingly, an overwhelming majority engage in efforts to protect their data: 86 percent of U.S. 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.[23]

238. K-12 education is compulsory, in part, to keep school-aged children off the labor market.

239. The EdTech data market is valued at nearly half a trillion dollars.

240. Thus, the information Instructure generates and collects as students use its products has significant economic value.

241. Instructure profits off of students by acquiring their sensitive and valuable personal information, which includes vastly more than mere demographic information perhaps necessary for obtaining consent, such as name, birth date, and email address.

242. Instructure then provides access to this data to more than one thousand third parties for a host of purposes, all unknown to students and their parents.

243. Instructure's actions have thus caused students economic injury.

244. By generating, collecting, using, and disclosing students' personal information without their knowledge or consent, Instructure has unfairly diminished the value of that information and students' future property interest without adequately compensating them.

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

246. Instructure's actions caused damage to and loss of students' property and

[23] Cisco, Consumer Privacy Survey (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf.

their right to control the dissemination and use of their personal information.

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

247. Instructure 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.

248. Recent research shows that nearly 80 percent of adults reported being very or somewhat concerned about how companies use data collected about adults,[24] and the number of those concerned about their online privacy is growing quickly.

249. Protective behaviors are on the rise, with 87 percent of U.S. adults using at least one privacy- or security-protecting tool online.[25]

250. 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%).[26]

251. Instructure has driven a wedge between school officials and parents, leaving parents reluctant to press their schools for information regarding Instructure's data practices or request that their children be alternatively accommodated.

252. Parents fear becoming adversarial with their children's schools and the possible repercussions they or their children might suffer if they are perceived as

---

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

[25] Olivia Sideot and Emily Vogels, What Americans Know About AI, Cybersecurity and Big Tech, Pew Research Center (August 17, 2023), https://www.pewresearch.org/internet/2023/08/17/what-americans-know-about-ai-cybersecurity-and-big-tech/.

[26] Polling Memo: Parents' Views on Children's Digital Privacy and Safety, Trusted Future (2022), https://trustedfuture.org/childrens-digital-privacy-and-safety/.

difficult or meddlesome, including stigmatization or retaliation. Instructure has thus chilled parental efforts to inquire about and object to its practices.

253. Children are thus particularly vulnerable and disempowered to protect themselves against Instructure's exploitative conduct.

254. Instructure should not be permitted to use schools as a shield against parent inquiry and concern and should be made to account for their data practices to those adversely affected by them.

255. Instructure forces children and their parents to choose between equal access to education on the one hand, and other basic rights, such as their rights to privacy and property, on the other.

V. Instructure's nonconsensual data practices are unfair and unlawful.

256. Instructure has generated massive profit through collection and analysis of children's personal information—without their parents' knowledge or consent, and without compensating them for actively and passively providing that valuable information.

257. This one-sided arrangement—whereby Instructure earns vast revenues each year from the personal information of children gathered through their compelled use of Instructure products, and all children 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 a public education.

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

VI. Plaintiff-Specific Allegations

A. Plaintiffs use Instructure products, which widely generate, collect, use, and share Plaintiffs' personal information.

259. Plaintiffs use Instructure products at their schools, including Canvas LMS.

260. Plaintiffs' use of Instructure products is mandatory.

261. Plaintiffs were unable to opt out of using Instructure products.

262. Those platforms are owned, controlled, and operated by Instructure.

263. Instructure has shared and continues to share Plaintiffs' data across its suite of products.

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

265. Instructure uses this information to develop, improve, and market its products and for other commercial purposes.

266. Instructure uses Plaintiffs' data generated and provided by schools to develop its analytics tools, which it sells to Plaintiffs' schools and school districts.

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

268. Instructure has enabled third parties to directly collect Plaintiffs' personal information.

B. Plaintiffs did not consent to Instructure's collection and use of their data.

269. Plaintiffs did not provide effective, informed, voluntary, and ongoing consent to Instructure's collection and use of their data for any purpose, let alone commercial purposes.

270. Instructure never notified Plaintiffs that their minor children were using Instructure products.

271. Plaintiffs were never provided material terms regarding Instructure's data practices, such as what personal information Instructure would collect, how it would be used, or who else would have access to it.

272. Plaintiffs' use of Instructure's products is compulsory.

273. Plaintiffs were not provided adequate consideration for Instructure's collection and use of their data.

274. Plaintiffs thus did not consent to Instructure's data practices.

275. 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 Instructure's level of surveillance and profiteering.

C. Instructure denied Plaintiffs access to, review of, and control over their data.

276. Plaintiff Saas requested access to the data Instructure collected from her child.

277. Instructure failed to provide Plaintiff Saas access to her child's data.

278. Plaintiff Saas was unable to obtain information relating to or arising from Instructure's collection or use of her child's data, either directly from Instructure or from her school.

279. On information and belief, Instructure has a policy of denying parents access to the data it collects about children and instead requiring that parents request access through their school administrators.

280. On information and belief, schools do not have access to or control over all the data that Instructure collects from and about students and their families.

281. To the extent schools do have access to such information, they are unable or unwilling to share all such information with students or their parents. Instructure

facilitates this obstruction by providing administrators the ability to limit what information students and parents may access.

282. Instructure may not absolve itself of its duty to provide parents access to their children's data by unilaterally purporting to shift that duty to schools.

D. Plaintiffs were harmed by Instructure's collection and use of their data.

283. Instructure's data practices harmed Plaintiffs in a number of material ways, as described herein.

284. Because Instructure refuses to disclose information critical to facilitating a meaningful understanding of its data practices, discovery is necessary to fully understand and identify the nature and details of these harms.

285. Instructure harmed Plaintiffs by invading their privacy.

286. Instructure's data practices and Plaintiffs' efforts to understand them and limit their harmful effects have compromised Plaintiffs' relationships with various school administrators, faculty, and staff.

287. Instructure has left Plaintiffs' personal and private information vulnerable to security risks, including identity theft.

288. Instructure harmed Plaintiffs by diminishing the value of their data.

289. Instructure harmed Plaintiffs by denying them, or having a policy of denying them, access to their own data.

290. Instructure harmed Plaintiffs by denying them, or having a policy of denying them, control over their own data.

291. Instructure harmed Plaintiffs by using their data to build intimate digital dossiers about them, and by using and disclosing those dossiers to untold third parties for untold purposes.

292. Instructure 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.

293. Instructure harmed Plaintiffs by failing to compensate them for their property or labor, which have fueled its highly lucrative business.

294. Plaintiffs are not fully aware of how they have been harmed by Instructure's nonconsensual data practices because Instructure has denied them access to the information necessary to determine the full extent of those harms.

CLASS ACTION ALLEGATIONS

295. Plaintiffs bring this class action pursuant to Rules 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure on behalf of themselves and all other similarly situated.

296. Plaintiffs seek to represent a nationwide class of students ("Nationwide Class") defined as:

> All persons in the United States who attend or attended a K-12 school who used Instructure K-12 school-marketed products.

297. Plaintiffs M.C. 1 and M.C. 2 seek to represent a state-only subclass of students ("California Subclass") under the law of the State of California defined as:

> All persons in California who attend or attended a K-12 school who used Instructure K-12 school-marketed products.

298. In addition, and in the alternative to the Nationwide Class, Plaintiffs reserve the right to seek leave to amend the complaint to represent state subclasses under the laws of 50 states.

299. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

300. The Nationwide Class and California Subclass are collectively referred to herein as the "Classes." Members of both Classes are collectively referred to herein as "Class members."

301. Excluded from the Classes 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; (3) persons who properly and timely request exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel, Classes' counsel, and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded person.

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

303. **Numerosity**: Members of the Classes are so numerous that joinder of all members is impracticable. The exact size of the Classes and the identities of the members of the Classes are readily ascertainable in or through Instructure's records.

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

305. **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 privacy violations. Plaintiffs and their counsel have no interest that is in conflict with or otherwise antagonistic to the interests of the other members of the Classes. 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.

306. **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 Instructure obtained effective consent to generate, obtain, use, and disclose the personal and private information of the members of the Classes;

b. Whether Instructure led the members of the Classes to believe, either directly or through school personnel, that their data and their privacy would be protected;

c. Whether Instructure represented that members of the Classes could control what data were intercepted, received, or collected by Instructure;

d. Whether Instructure actually protected the data and privacy of members of the Classes;

e. Whether Instructure's practice of intercepting, receiving, or collecting users' data violated state or federal privacy laws;

f. Whether Instructure's practice of intercepting, receiving, or collecting users' data violated anti-wiretapping laws;

g. Whether Instructure's practice of intercepting, receiving, or collecting users' data violated any other state or federal tort laws;

h. Whether Plaintiffs and members of the Classes are entitled to declaratory or injunctive relief to enjoin the unlawful conduct alleged herein; and

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

307. **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 members of the Classes have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Classes to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

308. 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.

TOLLING OF THE STATUTE OF LIMITATIONS

309. Any applicable statute(s) of limitations have been tolled by Instructure's and its affiliates' knowing and active concealment and denial of the facts alleged herein. Plaintiffs and members of the Classes could not have reasonably discovered the true nature of Instructure's data-harvesting scheme because Instructure purposely concealed it. Plaintiffs' claims were thus tolled under the discovery rule.

A. Discovery rule

310. The causes of action alleged herein did not accrue until Plaintiffs and members of the Classes discovered or could have discovered Instructure's data-harvesting scheme.

311. As alleged above, Plaintiffs and members of the Classes had no way of knowing about Instructure's data-harvesting scheme. Instructure concealed the scheme while simultaneously claiming that it protects student and parent data and privacy.

312. To this day, Instructure fails to disclose the full extent of, and risks associated with, its data-harvesting scheme.

313. Within any applicable statutes of limitation, Plaintiffs and members of the Classes could not have discovered, through the exercise of reasonable diligence, that Instructure was concealing the conduct complained of herein and misrepresenting the nature of its business.

314. Plaintiffs and members of the Classes did not know facts that would have caused a reasonable person to suspect that there was a data-harvesting scheme that would result in a private corporation collecting, manipulating, and monetizing every aspect of their children's lives and their own interactions with their children's schools and school districts. Instructure also withheld any and all information that would give a reasonable person knowledge of the data-harvesting scheme and disclaimed that it unlawfully monetized data about and belonging to Plaintiffs and members of the Classes.

315. For ordinary consumers, the existence of the data-harvesting scheme is still unknown. For these reasons, all applicable statutes of limitation have been tolled by operation of the discovery rule with respect to the claims in this litigation.

B. Fraudulent concealment

316. As an entity entrusted with sensitive, personal student and parent data, Instructure was under a continuous duty to disclose to Plaintiffs and members of the Classes the existence of the data-harvesting scheme.

317. Instructure was and is under a continuing duty to disclose to Plaintiffs and the members of the Classes what data it tracked, how that data is stored, how long it is retained, with whom it is shared, how it is manipulated, and how it is monetized.

318. Instead of disclosing this information, Instructure kept students and parents in the dark about its data-harvesting scheme and purposely misled parents and children, as well as schools and school districts, about how their data and other sensitive information was being collected and used by Instructure and others.

319. Plaintiffs and members of the Classes were not at fault for failing to discover the existence of Instructure's data-harvesting scheme.

320. This ignorance of the existence of Instructure's data-harvesting scheme is common across each Plaintiff and member of the Classes.

321. Due to Instructure's active concealment throughout the time period

relevant to this action, all applicable statutes of limitation have been tolled.

322. Instructure was and is under a continuous duty to disclose its data-harvesting scheme to Plaintiffs and members of the Classes. Instructure failed to disclose the existence of its data-harvesting scheme and actively concealed how it was using data and other sensitive information about and belonging to Plaintiffs and members of the Classes. Plaintiffs and members of the Classes reasonably relied upon Instructure's knowing and affirmative representations and/or active concealment of these facts. Based on the foregoing, Instructure is estopped from relying on any statutes of limitation in defense of this action.

CAUSES OF ACTION

Count I: Violation of 42 U.S.C. § 1983 – Fourth Amendment

(*On behalf of Plaintiffs and the Nationwide Class*)

323. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

324. To state a claim under 42 U.S.C. section 1983, a plaintiff must allege that the defendant, acting under color of law, deprived the plaintiff of a federally protected right.

325. The ultimate issue in determining whether a person is subject to suit under section 1983 is the same question posed in cases arising under the Fourteenth Amendment, which is whether the alleged infringement of federal rights is fairly attributable to the government.

326. Instructure engages in the conduct described herein with the authority of state and local government or in excess of that authority.

327. Instructure's conduct as described herein is pursuant to, or purportedly pursuant to, contracts with public schools and school districts.

328. Public schools and schools districts contract for Instructure's services using government funds.

329. Instructure deems itself a "school official" under federal law for purposes of the conduct described herein.

330. Instructure has been authorized by governmental entities to perform a function that is traditionally and exclusively a public function performed by the government, namely, the collection and management of public-school-related data, including education records and other student information.

331. Because of the sensitive nature of the information Instructure takes from children and the privacy rights associated therewith, access to such information is highly restricted and is subject to state and federal regulation. Therefore, access to such information is thus traditionally and exclusively managed only by authorized governmental entities. The law prohibits private entities from accessing such information except under strictly limited and narrow circumstances.

332. As a state actor with access to the personal and private information of K-12 students, Instructure owes a duty of care to those students and their parents, including Plaintiffs and Nationwide Class members.

333. Children do not forgo their Fourth Amendment rights by attending school as is their right and duty.

334. Instructure engages in conduct and employs policies, as described herein, that violate the constitutional rights of Plaintiffs and Nationwide Class members, including their Fourth Amendment right to be free from unreasonable searches and seizures and right to privacy.

335. Instructure itself acknowledges that students have a right to privacy, which it describes as "the right to be left alone, or freedom of interference or intrusion."

336. Instructure has far exceeded any legitimate authority it has to act on the government's behalf in performing a public function and unduly intruded upon the rights of Plaintiffs and Nationwide Class members.

337. Instructure's data practices, policies, technologies, and third-party data-

sharing agreements are not designed, controlled, or monitored by schools and school districts.

338. Instructure exercises considerable discretion in collecting, storing, using, and disclosing student data independent and separate from that of schools and school districts.

339. Instructure does not merely follow government specifications in its generation, collection, use, and disclosure of student data.

340. Instructure's surreptitious and persistent surveillance of Plaintiffs' and Nationwide Class members' activity as they use and interact with its products as described herein is a violation of their Fourth Amendment rights.

341. Instructure's persistent, indiscriminate, maximally intrusive surveillance and data practices are not justified or outweighed by any legitimate governmental interest.

342. Instructure's nonconsensual and surreptitious taking and using personal and private information of Plaintiffs and Nationwide Class members for its own financial gain as described herein is a violation of Plaintiffs' and Nationwide Class members' Fourth Amendment rights.

343. Instructure's policies that govern and authorize its sweeping generation and extraction of the personal and private information of Plaintiffs and Nationwide Class members are not narrowly tailored to achieve any legitimate governmental interest.

344. No compelling government interest outweighs Instructure's violations of Plaintiffs' and Nationwide Class members' constitutional rights.

345. Instructure is therefore liable to Plaintiffs and Nationwide Class members for their costs and fees, including attorney fees under 42 U.S.C. section 1988.

Count II: Violation of 42 U.S.C. § 1983 – Fourteenth Amendment
(*On behalf of Plaintiffs and the Nationwide Class*)

346. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

347. To state a claim under 42 U.S.C. section 1983, a plaintiff must allege that the defendant, acting under color of law, deprived the plaintiff of a federally protected right.

348. The ultimate issue in determining whether a person is subject to suit under section 1983 is the same question posed in cases arising under the Fourteenth Amendment, which is whether the alleged infringement of federal rights is fairly attributable to the government.

349. Instructure engages in the conduct described herein with the authority of state and local government or in excess of that authority.

350. Instructure's conduct as described herein is pursuant to, or purportedly pursuant to, contracts with public schools and school districts.

351. Public schools and school districts contract for Instructure's services using government funds.

352. Instructure deems itself a "school official" under federal law for purposes of the conduct described here.

353. Instructure has been authorized by governmental entities to perform a function that is traditionally and exclusively a public function performed by the government, namely, the collection and management of public-school-related data, including education records and other student information.

354. Because of the sensitive nature of such information and the privacy rights associated therewith, access to such information is highly restricted and is subject to state and federal regulation. Therefore, access to such information is thus traditionally and exclusively managed only by authorized governmental entities. The law prohibits

private entities from accessing such information except under strictly limited and narrow circumstances.

355. As a state actor with access to the personal and private information of K-12 students, Instructure owes a duty of care to those students and their parents.

356. Children do not forgo their Fourteenth Amendment rights by attending school as is their right and duty.

357. Instructure acknowledges that student "data privacy is a fundamental right[.]"

358. Instructure engages in conduct and employs policies that violate the constitutional rights of Plaintiffs and Nationwide Class members, including their Fourteenth Amendment right to privacy.

359. Instructure's nonconsensual taking and using of personal and private information of Plaintiffs and Nationwide Class members for its own financial gain as described herein violates their Fourteenth Amendment rights.

360. The information that Instructure generates and extracts from Plaintiffs and Nationwide Class members is information that is constitutionally protected. As Instructure states, "student data is even more sensitive than general personal data[.]"

361. Plaintiffs and Nationwide Class members have an interest in avoiding disclosure of their personal matters and information.

362. The indiscriminate and automatic generation, collection, and dissemination of the personal and private information of Plaintiffs and Nationwide Class members to an unbounded number of unknown, undisclosed entities violate their constitutional rights.

363. The policies that govern and authorize Instructure's sweeping generation, extraction, and disclosure of the personal and private information of Plaintiffs and Nationwide Class members are not narrowly tailored to achieve any legitimate governmental interest.

364. The privacy interests at issue—and Instructure's infringement thereof—are of constitutional importance.

365. Instructure has far exceeded any authority it has to act under the color of law on behalf of schools and school districts in the collection of the personal and private information of Plaintiffs and Nationwide Class members.

366. Instructure's data practices, policies, technologies, and third-party data-sharing agreements are not designed, controlled, or monitored by schools and school districts.

367. Instructure exercises considerable discretion, independent of schools and school districts, in collecting, storing, using, and disclosing Plaintiffs' and Nationwide Class members' protected information.

368. Instructure does not merely follow government specifications in its generation, collection, use, and disclosure of Plaintiffs' and Nationwide Class members' protected information

369. Instructure does not employ adequate safeguards, in practice or policy, to prevent further unauthorized disclosure of Plaintiffs' and Nationwide Class members' protected information.

370. Instructure's data practices and policies expose Plaintiffs' and Nationwide Class members' private information to significant risks, including the risk of identity theft.

371. Instructure admits that "[s]tudents, especially younger children, are not yet equipped to weigh the potential benefits and risks of data loss."

372. Instructure's denial of, and policy of denying, Plaintiffs' and Nationwide Class members' access to their own personal and private information violates their constitutional rights.

373. Instructure's denial of, and policy of denying, Plaintiffs' and Nationwide Class members' ability to control their own personal and private information violates

their constitutional rights.

374. These harms are exacerbated by the mandatory and surreptitious nature of Instructure's products and data practices, and their use against children in a compulsory environment.

375. Any governmental interest that is served by Instructure's invasive, exploitative data practices does not outweigh the rampant violations of Plaintiffs' and Nationwide Class members' privacy rights inflicted by Instructure's practices.

376. Instructure is therefore liable to Plaintiffs and Nationwide Class members for their costs and fees, including attorney fees under 42 U.S.C. section 1988.

Count III: Violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631, 632
(On behalf of California Plaintiffs and the California Subclass)

377. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

378. CIPA is codified at Cal. Penal Code sections 630–638. The purpose of CIPA is stated as follows:

> 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.

Cal. Penal Code § 630.

379. Cal. 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[.]

380. Cal. 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[.]

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

382. Instructure designed, contrived, and effectuated its scheme to track users in California.

383. Instructure's non-consensual tracking of the California Plaintiffs' and California Subclass members' internet communications was without authorization and consent from the California Plaintiffs and California Subclass members. The interception by Instructure in the aforementioned circumstances was unlawful and tortious.

384. The following items constitute machines, instruments, or contrivances under CIPA, and even if they do not, Instructure'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 Instructure used to track California Plaintiffs' and California Subclass members' communications;

b. The California Plaintiffs' and California Subclass members' browsers and mobile applications;

c. The California Plaintiffs' and California Subclass members' computing and mobile devices;

d. Instructure's servers that collect, maintain, and store California Plaintiffs' and California Subclass members' data;

e. The computer codes and programs used by Instructure to effectuate its tracking and interception of the California Plaintiffs' and California Subclass members' communications; and

f. The plan Instructure carried out to effectuate its tracking and interception of the California Plaintiffs' and California Subclass members' communications.

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

386. Instructure permitted numerous third parties to surreptitiously and unlawfully intercept protected communications belonging to California Plaintiffs and California Subclass members.

387. California Plaintiffs and California Subclass 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 personal and private information.

388. Pursuant to Cal. Penal Code section 637.2, California Plaintiffs and California Subclass members have been injured by the violations of Cal. 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 IV: Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code §§ 502, *et seq*.
(On behalf of California Plaintiffs and the California Subclass)

389. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

390. Cal. 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."

391. Plaintiffs and California Subclass members' devices on which they accessed Instructure's services, including computers, smart phones, and tablets, constitute computers or "computer systems" within the meaning of CDAFA. *Id*. § 502(b)(5).

392. Instructure violated Cal. Penal Code section 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using California Plaintiffs' and California Subclass members' data.

393. Instructure effectively charged California Plaintiffs and California Subclass members and was enriched by acquiring their sensitive and valuable personal information without permission and using it for Instructure's own financial benefit to advance its business interests.

394. California Plaintiffs and California Subclass members retain a stake in the profits that Instructure earned from the misuse of their activity and personally identifiable information because, under the circumstances, it is unjust for Instructure to retain those profits.

395. Instructure accessed, copied, took, analyzed, and used from California

Plaintiffs' and California Subclass members' computers in and from the State of California, where Instructure marketed and sold its products. Accordingly, Instructure caused the access of their computers in California and is therefore deemed to have accessed their computers in California.

396. As a direct and proximate result of Instructure's unlawful conduct within the meaning of Cal. Penal Code section 502, Instructure has caused loss to California Plaintiffs and California Subclass members and has been unjustly enriched in an amount to be proven at trial.

397. California Plaintiffs and California Subclass members seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

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

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

Count V: Violation of California's Unfair Competition Law ("UCL") Cal. Bus. & Prof. Code § 17200, *et seq*.
(*On behalf of California Plaintiffs and the California Subclass*)

400. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

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

402. 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.

403. Instructure's conduct violated the spirit and letter of these laws, which protect property, economic, and privacy interests and prohibit unauthorized disclosure and collection of private communications and personal information.

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

405. To establish liability under the "unfair" prong, California Plaintiffs and California Subclass 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 the negative impact of Instructure's practices on school-aged children and their parents far outweighs the reasons, justifications, and motives of Instructure.

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

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

408. California Plaintiffs and California Subclass members have suffered injury-in-fact, including the loss of money or property as a result of Instructure's unfair and unlawful practices, the unauthorized disclosure and taking of their personal information which has value as demonstrated by its use and sale by Instructure. California Plaintiffs and California Subclass members have suffered harm in the form

of diminution of the value of their private and personally identifiable data and content.

409. Instructure's actions caused damage to and loss of California Plaintiffs' and California Subclass members' property right to control the dissemination and use of their personal information and communications.

410. Instructure reaped unjust profits and revenues in violation of the UCL. This includes Instructure's profits and revenues from their sale and licensing of its products, which Instructure develops, delivers, maintains, and improves using the personal and private information of California Plaintiffs and California Subclass members, as well as through data-sharing agreements with innumerable third parties. California Plaintiffs and the California Subclass members seek restitution and disgorgement of these unjust profits and revenues.

Count VI: Violation of Cal. Civ. Code § 52.1 (Tom Bane Civil Rights Act)
(*On behalf of the California Plaintiffs and California Subclass*)

411. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

412. The Bane Act punishes any "person or persons, whether or not acting under color of law, [who] interferes by threat, intimidation, or coercion, or attempts to interfere by threat, intimidation, or coercion, with the exercise or enjoyment by any individual or individuals of rights secured by the Constitution or laws of the United States, or of the rights secured by the Constitution or laws of this state." Cal Civ. Code § 52.1(a).

413. Plaintiffs' and Class members' expectation of privacy is deeply enshrined, among other laws, 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 principal purpose of the constitutional right to privacy was to protect

against unnecessary information gathering, use, and dissemination by public and private entities.

414. Instructure interfered or attempted to interfere with the California Plaintiffs' and the California Subclass members' state and federal rights as described and alleged herein by coercion in conditioning a child's receipt and use of required educational services on the provision of vast troves of their personal and private information.

415. Instructure exploited the inherently coercive nature of the compulsory setting of K-12 education in purporting to obtain parental consent—or conscripting schools to obtain parental consent—to its exploitative data practices.

416. By its coercive conduct, Instructure interfered or attempted to interfere with the California Plaintiffs' and the California Subclass members' right to a free education, right to privacy, and right to be compensated for their property and labor from which Instructure benefited commercially.

417. Instructure engaged in such conduct with the intent to violate, or in reckless disregard of violating, the California Plaintiffs' and the California Subclass members' rights.

418. Instructure's conduct violates clearly established statutory and constitutional rights of which a reasonable person would have known.

419. In acting as alleged herein, Instructure acted knowingly, willfully, and maliciously, and with reckless and callous disregard for the California Plaintiffs' and the California Subclass members' clearly established and constitutionally protected rights, including their fundamental rights to privacy, justifying an award of punitive damages in an amount sufficient to punish Instructure and discourage others from engaging in similar gross abuse of the public trust and governmental power.

Count VII: Invasion of Privacy—Public Disclosure of Private Facts
(On Behalf of Plaintiffs and the Nationwide Class)

420. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

421. The State of 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.

422. Instructure, as a matter of course, disclosed Plaintiffs' and Nationwide Class members' personal information to its vast network of partners, as described herein. The recipients of Plaintiffs' and Nationwide Class members' personal information because of Instructure's disclosures are so numerous that they amount to public disclosures.

423. Moreover, Instructure's creation and disclosure of intimate digital dossiers containing Plaintiffs' and Nationwide Class members' personal information further constitutes public disclosures of that information.

424. The contents of the personal information that Instructure 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. Instructure's disclosure of this information would be highly offensive and objectionable to a reasonable person of ordinary sensibilities.

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

a. The Fourth Amendment right to privacy contained on school-issued

and/or personal computing devices, including all of their activity on their devices;

b. The Fourteenth Amendment right to informational privacy;

c. COPPA;

d. CIPA;

e. CDAFA;

f. The Bane Act; and

g. Common-law expectations of privacy.

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

427. Instructure's actions constituted a serious invasion of privacy in that it:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including web search, browsing histories, personal and private communications and content, and other activities to which Instructure had no legitimate basis for accessing;

b. Invaded a zone of privacy protected by the Fourteenth Amendment, namely the right to privacy in information contained on personal computing devices, including web search, browsing histories, personal and private communications and content, and other activities to which Instructure had no legitimate basis for accessing;

c. Violated federal and state statutes, including COPPA, CIPA, CDAFA, and the Tom Bane Act;

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

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

f. Further violated Plaintiffs' and Nationwide Class members' reasonable expectation of privacy via Instructure's review, analysis, and subsequent use of Plaintiffs' and Nationwide Class members' activity that was considered sensitive and confidential.

428. Committing these acts against Plaintiffs and Nationwide Class members alike constitutes an egregious breach of social norms that is highly offensive, particularly given Instructure's specific targeting of school-aged children in a compulsory setting for data extraction and exploitation.

429. Instructure's surreptitious and unauthorized tracking of Plaintiffs' and Nationwide Class members' activity constitutes an egregious breach of social norms that is highly offensive, particularly given that Instructure's K-12-marketed products were represented as tools to assist with the education of children.

430. Taking this information through deceit is highly offensive behavior, and Instructure lacked any legitimate business interest in tracking Plaintiffs and Nationwide Class members without their consent.

431. Instructure's invasions of Plaintiffs' and Nationwide Class members' privacy were with oppression, fraud, or malice.

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

Count VIII: Invasion of Privacy—Intrusion Upon Seclusion
(*On behalf of Plaintiffs and the Nationwide Class*)

433. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

434. 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.

435. Instructure intentionally intruded into Plaintiffs' and Nationwide Class

members' private affairs in a highly offensive manner through its systematic and pervasive collection, accessing, downloading, transferring, selling, storing and use of Plaintiffs' and Nationwide Class members' private information and data.

436. Plaintiffs and Nationwide Class members maintained a reasonable expectation of privacy interest in their personal information absent consent to tracking and collection practices. Plaintiffs and Nationwide Class members never consented—and in the case of Instructure school-licensed products, never even had the opportunity to consent—to Instructure's data practices. The reasonableness of this expectation is reflected in longstanding custom and practice; security measures intended to prevent unauthorized access to personal information, especially concerning young children; state, federal, and international laws protecting a right to financial privacy; and the privacy policies and other assurances of protection by applications that use Instructure discussed herein, among other indicia.

437. Plaintiffs and Class members could not reasonably expect that Instructure would collect, store, manipulate, and monetize such voluminous, far-reaching, and sensitive categories of personal information, prevent Plaintiffs and Nationwide Class members from reviewing or controlling that information, and use that information in ways that were harmful to Plaintiffs and Nationwide Class members.

438. Individuals also maintain a reasonable expectation of privacy when they are using products in a compulsory environment such as public schools. Instructure's collection of Plaintiffs and Nationwide Class members' information while logged into Instructure products was also unreasonable.

439. Instructure's collection and use of children's data and personal information without the knowledge or consent of those children or their parents is highly offensive to an ordinary reasonable person.

440. Instructure's collection and use of parent data and personal information without the knowledge or consent of parents is highly offensive to an ordinary

reasonable person.

441. Instructure's intrusions upon Plaintiffs' and Nationwide Class members' private affairs and concerns are highly offensive to an ordinary reasonable person, especially considering (a) the highly sensitive and personal nature of Plaintiffs' and Nationwide Class members' personal information and data; (b) the extensive scope of data obtained by Instructure, including years of historical data; (c) Instructure's intent to profit from Plaintiffs' and Nationwide Class members' data by selling it outright (*e.g.*, back to schools, its "customers," and myriad other third parties) and using it to develop and market its products and services; (d) Instructure's use of subterfuge to intrude into Plaintiffs' and Nationwide Class members' electronic devices for the purpose of collecting their data; (e) the surreptitious and unseen nature of Instructure's data collection with respect to consumers, and (f) Instructure's failure to obtain valid consent.

442. Instructure's conduct would be highly offensive to a reasonable person, particularly given Instructure's extensive and false public statements regarding its commitment to user privacy and given that Instructure designs products to be used by children, including young children. The manner of the invasion—collection through students' use of education tools in a compulsory setting—is also highly offensive.

443. Instructure's invasions of privacy caused Plaintiffs and Nationwide Class members the following damages:

a. Nominal damages;

b. The diminution in value of Plaintiffs' and Nationwide Class members' private information;

c. The loss of privacy due to Instructure rendering no longer private the sensitive and confidential information that Plaintiffs and Nationwide Class members intended to remain private; and

d. Instructure took something of value from Plaintiffs and Nationwide Class members—their personal information and data—and derived benefits

therefrom without Plaintiffs' and Nationwide Class members' knowledge or consent and without Instructure sharing the fair benefit of such value with them.

444. Instructure's invasions of Plaintiffs' and Nationwide Class members' privacy were with oppression, fraud, or malice.

445. As a result of Instructure's invasions of privacy, Plaintiffs and Nationwide Class members seek actual damages, compensatory damages, restitution, disgorgement, general damages, nominal damages, unjust enrichment, punitive damages, and any other relief the Court deems just.

Count IX: Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

446. Plaintiffs incorporate by reference paragraphs 1 through 322 as though fully set forth herein.

447. Instructure has unjustly received benefits at the expense of Plaintiffs and Nationwide Class members.

448. Instructure acquired and compromised troves of personal data that rightfully belong to Plaintiffs and Nationwide Class members without effective consent through intentionally deceptive practices conducted in connection with students' use of Instructure's products.

449. Instructure has derived profits and other tangible benefits from its improper collection, use, and disclosure of children's data.

450. Without collecting children's data without effective consent, Instructure could not have grown its business, acquired numerous other tangible and intangible assets, developed other apps, gone public in 2021 at a $2.9 billion valuation, and been acquired by Kohlberg Kravis Roberts in November 2024 in an all-cash deal valuing the company at $4.8 billion.

451. Instructure has also directly and substantially profited from its use,

storage, aggregation, and sale of Plaintiffs' and Nationwide Class members' data. Indeed, Plaintiffs' and Nationwide Class members' data is the fuel that powers Instructure's ever-growing "Ed-cosystem" products and services, the core business of Instructure. Without Plaintiffs' and Nationwide Class members' personal information unlawfully taken by Instructure, Instructure would cease to operate in its current form.

452. These benefits were the expected result of Instructure acting in its pecuniary interests at the expense of its users.

453. In exchange for these benefits to Instructure, Plaintiffs and Nationwide Class members received nothing but educational services to which they were already legally entitled and required to receive.

454. To benefit its bottom line, Instructure deprived Plaintiffs and Nationwide Class members of their property, security, privacy, and autonomy.

455. Instructure harmed Plaintiffs and Nationwide Class members by, among other harms, subjecting them to commercial manipulation and continuous surveillance; invading their privacy; denying their due process rights by subjecting them to opaque, unreviewable data practices; forcing them to choose between their right to an education and other fundamental rights; and failing to compensate them for their property and labor.

456. Plaintiffs and Nationwide Class members did not consent to Instructure's taking of their information and using it for Instructure's or other third parties' commercial gain.

457. There is no justification for Instructure's enrichment. It would be inequitable, unconscionable, and unjust for Instructure to be permitted to retain these benefits because the benefits were procured because of and by means of their wrongful conduct, and at the expense of children's privacy and property.

458. Plaintiffs and Nationwide Class members seek an order compelling Instructure to disgorge the profits and other benefits it has unjustly obtained.

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

460. Plaintiffs and Nationwide Class Members may not have an adequate remedy at law against Instructure, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

RELIEF REQUESTED

WHEREFORE, Plaintiffs respectfully request the Court enter judgment in their favor and against Instructure 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: March 27, 2025

Respectfully submitted,

By: */s/ Melisa A. Rosadini-Knott*

Melisa A. Rosadini-Knott
(California Bar No. 316369)
PEIFFER WOLF CARR KANE CONWAY & WISE LLP
3435 Wilshire Blvd., Ste. 1400
Los Angeles, CA 90010-1923
323-982-4109
mrosadini@peifferwolf.com

Brandon M. Wise*
PEIFFER WOLF CARR KANE CONWAY & WISE LLP
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
(314) 833-4825
bwise@peifferwolf.com

Andrew R. Tate*
PEIFFER WOLF CARR KANE CONWAY & WISE LLP
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
(314) 669-3600
atate@peifferwolf.com

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

Lori G. Feldman*
GEORGE FELDMAN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, NY 10520
(917) 983-9321
LFeldman@4-Justice.com
eService@4-justice.com

Brittany L. Sackrin*
GEORGE FELDMAN MCDONALD, PLLC
9897 Lake Worth Road, Suite 302
Lake Worth, Florida 33467
(561) 232-6002
BSackrin@4-Justice.com

eService@4-Justice.com

Karen Dahlberg O'Connell*
ALMEIDA LAW GROUP LLC
157 Columbus Ave, 4th Floor
New York NY 10023
(347) 395-5666
karen@almeidalawgroup.com

Britany A. Kabakov*
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
(708) 529-5418
britany@almeidalawgroup.com

* *pro hac vice* forthcoming

Counsel for Plaintiffs and the Proposed Classes

ClassAction.org
