

FILED  
2026 AUG 14 04:16 PM  
KING COUNTY  
SUPERIOR COURT CLERK  
E-FILED  
CASE #: 26-2-26702-2 SEA

IN THE SUPERIOR COURT FOR THE STATE OF WASHINGTON  
IN AND FOR THE COUNTY OF KING

A.W., M.W., H.W.1, and H.W.2, minors, by  
and through their parent and legal guardian  
ELLA WILLIAMS, individually and on  
behalf of all others similarly situated,

Plaintiffs,

v.

MICROSOFT CORPORATION,

Defendant.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT FOR:**

- 1. Violation of Wash. Rev. Code Ann. §§ 19.86.020**
- 2. Invasion of Privacy-Intrusion Upon Seclusion**
- 3. Unjust Enrichment - Quasi Contract**
- 4. Violation of Wash. Rev. Code §§ 19.373, *et seq.***

**JURY TRIAL DEMANDED**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

## **I. INTRODUCTION**

1. Defendant Microsoft Corporation (“Microsoft”) markets, sells, and provides digital products to Washington K-12 public schools claiming that (1) its products are exclusively designed to help support school personnel and students and (2) it collects and uses student data only for educational purposes and under the schools’ direct control.

2. In reality, through its K-12 products, Microsoft operates a massive student-data harvesting apparatus far beyond what is necessary to provide education services to schools that exceeds both schools’ control and parents’ expectations. Microsoft collects, extracts, and generates vast troves of student data, converts that data into hyper-detailed psychographic profiles of students, and uses that data for its own commercial and other purposes, enriching itself at students’ expense.

3. Schools have always been authorized to collect and use certain student information to provide education services; they may even enlist the services of private companies in doing so. But that authority is not unbounded: it is limited by state and federal laws that require fair and honest business practices and that protect the privacy rights of students and minors, and the rights of parents to access, control, and protect their children’s personal information.

4. Microsoft, however, acts as though no such boundaries exist. It acts as though it alone—not parents and not even schools—has the right to determine the type and amount of personal information it can take from students and the ways in which it can use it.

5. Microsoft deploys its expansive data-mining operation through its systems of products, within which students are captive participants because they are required to use the products as part of their compulsory education.

6. The products at issue include Microsoft’s personal computers, operating system, browser, search engine, and cloud-based software suite of applications, tools, and services.

7. A student’s Microsoft account becomes the default environment of virtually every aspect of the child’s education, including storage and creation of the student’s digital identity and history, access to school resources and information, classroom participation, creation of school-

1 related content, communications, performance and behavioral analytics, diagnostic outputs from  
2 assessments, and school administrative logs.

3 8. Microsoft's data-harvesting apparatus spans every level of this system, transforming  
4 the classroom into an environment of persistent digital surveillance, data extraction, and algorithmic  
5 profiling.

6 9. The student data Microsoft collects includes education records provided by the  
7 school, such as student contact and demographic information, school and grade level, enrollment  
8 and attendance, grades and test scores, and disciplinary and health records. This information is highly  
9 sensitive and receives additional protection under federal law. But Microsoft collects many other  
10 categories of student data.

11 10. In addition to these sensitive records, Microsoft also collects student behavioral data,  
12 such as details of a student's web-browsing history and app usage, student search queries and results,  
13 student posts and communications, and the nature, substance, and context of the online content a  
14 student consumes. It even collects so-called "telemetric" student data, which is information about  
15 how a student's body physically interacts with her device and its digital features. That includes  
16 information such as when and how a student submits content, including school assignments; when  
17 and how quickly a student types and scrolls; how long she hovers over on-screen items; how and  
18 how often a student switches tabs; and what buttons she presses, when she presses them, and the  
19 order in which she presses them.

20 11. Beyond education records, behavioral data, and telemetric data, Microsoft also  
21 collects metadata about these categories of data, which is the technical layer where product analytics  
22 and student behavior overlap. Even when steps are taken to de-identify student data, the metadata is  
23 so structurally distinct that it provides a precise blueprint of user attention, reading patterns, and  
24 device usage.

25 12. This quality and quantity of student information far exceed what a parent would  
26 reasonably expect to be collected from their child at school without the parent's knowledge or  
27 consent.

1           13.     Contrary to what parents and others would expect, Microsoft does not merely collect  
2 the data and then securely store it on behalf of schools.

3           14.     **First**, Microsoft uses this data to generate so-called “insights” about students.  
4 Processing all the data that it has obtained about and extracted from students through its proprietary  
5 algorithms, Microsoft generates diagnostic and predictive inferences about every aspect of a student,  
6 including her cognitive and skill proficiency, learning activity, attendance and participation, behavior  
7 and engagement, social environment (including teacher, peer, and familial relationships), and her  
8 emotions and well-being.

9           15.     **Second**, these inferences are then aggregated into a persistent digital profile of the  
10 student that constitutes a lasting record of every aspect of the student. Schools use these profiles to  
11 purportedly better understand students, influence their behavior and experiences, and make  
12 consequential decisions affecting their lives. Further, Microsoft’s internet search engine uses  
13 information specific to individual users, including search history, location, and engagement, to  
14 determine the results each user sees. On information and belief, based on Microsoft’s documented  
15 design of its internet browser and search engine and its collection of student search and browsing  
16 data alleged herein, these same mechanisms operate on students’ school accounts, delivering results  
17 shaped by each student’s accumulated profile, thus atomizing students’ informational environment  
18 while enabling Microsoft to extract ever more data from students as they use the internet.

19           16.     **Third**, Microsoft exploits its educational mandate and exploits student data for a  
20 variety of commercial purposes, including generating robust student analytics that are  
21 disproportionate to the needs of schools and students and using them to build, improve, market, and  
22 deliver its own products and services.

23           17.     Although Microsoft states that schools control the realms of student data that  
24 Microsoft collects as students use its products, they do not—and indeed cannot. The most important  
25 data-extraction and processing activities occur inside Microsoft’s proprietary systems to which  
26 school personnel do not have access. Microsoft exploits this asymmetry in numerous ways described  
27 herein that benefit Microsoft at students’ expense.

1           18.     Critically, parents of K-12 students are not aware of, do not understand, and never  
2 consented to Microsoft's invasive data mining and profiling of their children.

3           19.     Microsoft's student-data practices far exceed those that parents would reasonably  
4 expect their children to be subjected to in the compulsory environment of K-12 education while  
5 using required school products without their consent.

6           20.     Privacy is a fundamental right. Children have a right to privacy in the information  
7 that is generated and taken from them, including when at school. Parents have a right to determine  
8 who may access that personal information and for what purpose, and the right to determine whether  
9 certain information is created in the first place—including the creation of intimate behavioral profiles  
10 of their children.

11          21.     While everyone has a fundamental right to privacy, children under 13 have additional  
12 statutory protections under the Children's Online Privacy Protection Act ("COPPA"). Microsoft  
13 intentionally and knowingly violates COPPA by failing to provide parents of children under 13 with  
14 notice of its data practices or obtain their consent and by actively concealing its practices by denying  
15 parents access to the data it collects about their children.

16          22.     Further, Washington enacted the My Health My Data Act (RCW §§ 19.373, *et seq.*)  
17 (the "MHMDA") precisely to provide heightened protections for Washingtonian's health data and  
18 ensure their right to privacy. The MHMDA imposes clear requirements and duties on regulated  
19 entities, including entities like Microsoft, to obtain affirmative consent before collecting consumer  
20 health data, maintain a consumer health data privacy policy that clearly identifies what health  
21 information is being collected and for what purpose, and establish data security practices that protect  
22 the confidentiality, integrity, and accessibility of consumer health data.

23          23.     Microsoft's data practices force students to entirely forgo their rights in order to  
24 receive the education to which they are legally entitled. And parents, by sending their children to  
25 school as is their right and duty, are forced to surrender their longstanding authority to make critical  
26 decisions about their children's personal information.

1           24.     Through its contracts with schools, Microsoft attempts to shift all legal responsibility  
2 for collecting and managing student data to schools. But the law does not enable Microsoft to avoid  
3 liability by contract for its commercial exploitation of student data.

4           25.     Microsoft must be held accountable for acting as though the rights of students and  
5 their parents do not exist.

6           26.     Plaintiffs are among the more than one million Washington schoolchildren whose  
7 personal information was unlawfully taken and used by Microsoft. Through this suit, they seek  
8 redress on behalf of themselves and on behalf of the other K-12 students harmed by Microsoft's  
9 exploitative data practices.

## 10                               **II.     JURISDICTION AND VENUE**

11           27.     This Court has jurisdiction over this cause of action under RCW § 2.08.010.

12           28.     This Court has personal jurisdiction over Microsoft because Microsoft is a  
13 Washington corporation headquartered in King County, Washington.

14           29.     Venue is proper in this Court pursuant to RCW § 4.12.020(3) and RCW § 4.12.025  
15 because Microsoft resides in King County, Washington.

## 16                               **III.     THE PARTIES**

17           30.     Plaintiff A.W. is a minor. At all relevant times, he has been a citizen of the state of  
18 Washington. A.W. attends high school in Spokane County in the Spokane Public Schools. As part of  
19 his schooling, he was required to access and use Microsoft Windows 10 and Windows 11, the  
20 Microsoft Edge web browser, Microsoft Outlook, Minecraft Education, and the Microsoft 365  
21 Education suite of applications, tools, and services, which he accessed and used from his school-  
22 issued laptop.

23           31.     Plaintiff M.W. is a minor. At all relevant times, he has been a citizen of the state of  
24 Washington. M.W. attends middle school in Spokane County in the Spokane Public Schools. As part  
25 of his schooling, he was required to access and use Microsoft Windows 11, the Microsoft Edge web  
26 browser, Microsoft Outlook, Minecraft Education, and the Microsoft 365 Education suite of  
27 applications, tools, and services, which he accessed and used from his school-issued laptop.

1           32. Plaintiff H.W.1 is a minor and under the age of 13. At all relevant times, he has been  
2 a citizen of the state of Washington. H.W.1 attends elementary school in Spokane County in the  
3 Spokane Public Schools. As part of his schooling, he was required to access and use Microsoft  
4 Windows 11, Minecraft Education, and the Microsoft Edge web browser, which he accessed and  
5 used from his school-issued laptop.

6           33. Plaintiff H.W.2 is a minor and under the age of 13. At all relevant times, he has been  
7 a citizen of the state of Washington. H.W.2 attends elementary school in Spokane County in the  
8 Spokane Public Schools. As part of his schooling, he was required to access and use Microsoft  
9 Windows 11, Minecraft Education, and the Microsoft Edge web browser, which he accessed and  
10 used from a school-issued device located on school property.

11           34. Ella Williams is the mother and legal guardian of Plaintiffs A.W., M.W., H.W.1, and  
12 H.W.2. At all relevant times, she has been a citizen of the state of Washington.

13           35. Defendant Microsoft is a Washington corporation. Its headquarters are located at One  
14 Microsoft Way, Redmond, Washington 98052.

#### 15                                   IV. FACTUAL ALLEGATIONS

16           36. Microsoft collects and generates vast troves of personal information belonging to  
17 more than one million Washington students, including Plaintiffs; creates deeply personal and  
18 sensitive profiles of each student; and provides and uses the data for predictive and other analytics  
19 that enrich Microsoft and influence the student in ways determined by Microsoft. It does all of this  
20 without effective consent in violation of federal and state law.

21           37. The products through which Microsoft collects student data and which are the subject  
22 of this Complaint include the following (collectively, “Products”):

- 23           a. **Microsoft Personal Computer (“PC”)** is a computer, including a laptop, running  
24 Microsoft’s Windows operating system.
- 25           b. **Microsoft Windows 10 and Windows 11** are each a series of operating systems that  
26 manage a computer’s hardware and software. They provide a graphical interface for  
27 Plaintiffs to interact with their computers, laptops, and tablets, and provide access to the  
Microsoft Edge internet browser and any applications and files on the device.
- c. **Microsoft 365 Education** is a cloud-based software suite that includes several

1 applications, tools, and services, including but not limited to Word (a word-processing  
2 application), Excel (a spreadsheet application for data organization and analysis),  
3 PowerPoint (a slideshow presentation application), Teams (a collaboration software  
4 allowing for video meetings, live chats, file sharing, and student responses to questions  
about their feelings and emotional states), and Outlook (an email service), which are all  
applications used by Plaintiffs.

5 d. **Microsoft Edge** is an internet browser with built-in learning and accessibility tools that  
6 is the default browser for Microsoft Windows and is also supported on Mac operating  
7 systems, iPhone and iPad operating systems, and Android tablets and phones. Its use is  
8 required by Plaintiffs' school districts, and Plaintiffs use it to access its search engine,  
**Bing**, to conduct Internet searches and access any of the web-based applications in  
Microsoft 365 Education.

9 e. **Microsoft Minecraft Education** is a game-based platform with a built-in lesson library  
10 that Plaintiffs use as part of their required schoolwork.

11 38. Plaintiffs' school district is one among a substantial majority of Washington school  
12 districts that require that students use one or more of the Products.

13 **A. Microsoft collects an enormous amount of student data.**

14 39. Microsoft collects vast troves of student data as students use its Products. The types  
15 of data it collects can be divided into three categories: student education records, behavioral data,  
16 and metadata.

17 **1. Student education records**

18 40. Education records collected by Microsoft include information such as a student's  
19 name, other identifying information, contact information, demographic information, grade level,  
20 school name, class roster, enrollment and attendance, assignments, grades, test results, recorded  
21 schoolwork, disciplinary records, and medical and health information. This data is typically input by  
22 school personnel, parents, or students themselves.

23 **2. Student behavioral data**

24 41. Student behavioral data extracted by Microsoft encompasses all measurable actions  
25 a student or system takes while a student engages with a physical product or digital service. It is data  
26 resulting from the continuous tracking of *what* students do and view online (conscious or active  
27 behavioral data) and *how* they do it (unconscious or telemetric behavioral data).

1                   **a. Active student behavioral data**

2           42.     An example of active student behavioral data is the student's internet browsing  
3 history, which includes data about a student's page views, the links a student clicks and interacts  
4 with, online search queries, advertisement preferences and interactions, and how long a student  
5 spends on a page. It also includes intentional student interaction and content engagement, such as  
6 online form submissions; shared content, video playback, media consumption, and app and software  
7 usage, such as clicking specific buttons, creating user accounts, or adjusting settings.

8           43.     Microsoft collects active student behavioral data through its Microsoft Edge product  
9 and through Bing, the default search engine within Edge in Windows 10 and the only search engine  
10 within Edge in Windows 11; its Microsoft 365 Education product and the applications and tools the  
11 students use within that product; and Microsoft Minecraft Education.

12           44.     Bing is intentionally designed to collect and analyze user data—most notably, search  
13 queries, click behavior, and contextual signals such as location, browser characteristics, and device  
14 configuration—as a core part of its algorithmic architecture. This design reflects a strategic decision  
15 to treat user interaction data as a key input for understanding searcher intent, improving the relevance  
16 of search results, and refining Bing's search functionality.

17           45.     Microsoft has admitted in public research papers and technical documentation that  
18 behavioral data generated through Bing—including search queries, clicks, and engagement  
19 signals—is used to inform machine-learning models that personalize rankings, refine autocomplete  
20 suggestions, and adjust result presentation based on prior engagement patterns. In an antitrust  
21 proceeding, *United States v. Google LLC*, testimony and exhibits from Microsoft representatives  
22 further confirmed that user clicks and engagement are used not merely as passive feedback but as  
23 predictive signals that shape Bing's learning algorithms and influence future search outputs. As  
24 Apple's senior vice president of machine learning and AI strategy noted when discussing Bing's lack  
25 of access to the iPhone userbase (due to Apple choosing Google as Safari's default search engine):  
26 "[n]ot having mobile search queries at scale is a huge liability for [Bing] since the most important  
27 search signal is [user] engagement."

1           46.     Crucially, this level of tracking is not necessary for a general-purpose search engine  
2 to function. Alternative search engines—such as DuckDuckGo and Startpage—operate without  
3 storing user-identifiable information, session data, or click-through history. These platforms  
4 demonstrate that effective search organization can be achieved through content-based ranking and  
5 real-time query analysis, without building behavioral dossiers or maintaining persistent identifiers.  
6 Unlike Bing, these services do not tie user queries to profiles or log activity over time, choosing  
7 instead to discard or anonymize click data entirely. This contrast underscores that Microsoft’s  
8 practices are not technologically essential but rather reflect a business model that prioritizes data  
9 monetization and product feedback over user privacy.

10                   **b. Telemetric student behavioral data**

11           47.     Telemetric student behavioral data refers to the automatic collection of usage and  
12 performance data from students as they use Microsoft’s Products. It captures the actions,  
13 interactions, and operations of students, systems, and devices in real-time, which serve as the  
14 underlying signals that chronicle “user journeys.” Microsoft automatically collects telemetric data  
15 by default in all of its Products.

16           48.     While Microsoft also collects systemic telemetric information like browsing history,  
17 application version, device type, operating-system information, service connectivity, crash reports,  
18 error signals, and feature performance, the student telemetric data it extracts includes intimate  
19 information about how a student physically uses and moves her body both intentionally and  
20 reflexively while using a device. Such data includes keystroke patterns and rhythms such as how  
21 quickly a student scrolls, types, and clicks; how she interacts with menus and toolbars; how long she  
22 hovers her mouse over items; her tab-switching behaviors; her error-correction patterns; how she  
23 navigates platforms; her scroll depth within apps and websites; and even how hard she presses  
24 buttons. It is a student’s “digital nervous system.”

25           49.     Microsoft tracks and collects this telemetric behavioral data by setting cookies within  
26 its Microsoft 365 Education product, as revealed by a forensic investigation conducted within a  
27 plaintiff’s Microsoft account. The investigation examined the Word, PowerPoint, Excel, Teams, and

1 Outlook apps within the Microsoft 365 Education product in the plaintiff’s account and revealed that  
2 Microsoft set numerous cookies (small files placed on a student’s browser to track her online  
3 activity) within the product, including cookies that serve as a universally unique user identifier (a  
4 randomly generated string of numbers unique to an individual and designed to track her activity over  
5 time and across multiple devices), as well as cookies related to telemetry, including “ai\_session”  
6 cookies that appeared to be associated with Microsoft’s artificial-intelligence operations.

7 50. For example, forensic testing from analysis of a Word document created in the online  
8 (browser) version of Word, revealed that Microsoft set 29 cookies on the browser while testing  
9 occurred, including “ai\_session” cookies and cookies related to telemetry. During the creation of the  
10 Word document, 56 calls—i.e., network requests sent by the application to Microsoft-controlled  
11 internet servers—were made over the course of 15 minutes to a “telemetry” domain or file name.

12 51. Testing of Microsoft’s other cloud-based applications revealed similar activity,  
13 including, but not limited to, the online versions of Excel and PowerPoint. Over the course of just  
14 15 minutes, those products were observed making dozens of calls to a telemetry domain or file name.

15 52. Microsoft also collects user-engagement telemetry through Bing, including  
16 timestamps, query reformulations, dwell time on clicked results, and identifiers that persist across  
17 sessions—allowing the platform to track a student’s behavior longitudinally and engage in cross-  
18 service profiling. This form of session-based telemetry is not incidental or purely diagnostic; rather,  
19 it is the product of a series of deliberate design choices that prioritize behavioral surveillance over  
20 student anonymity.

### 21 3. Student’s consumer health data

22 53. The student data Microsoft collects and generates includes consumer health data.  
23 Specifically, the data collected and generated by Microsoft includes students’ medical and health  
24 information. As one example, Microsoft’s Teams product includes social-emotional “check-in”  
25 features, such as Microsoft Reflect, which is deployed within Teams for Education. Through “check-  
26 ins,” students are prompted to report their feelings and emotional states (i.e., “I am feeling anxious  
27 today,” or “I am feeling overwhelmed today”), and students respond to such prompts as part of

1 required schoolwork. Microsoft's Products further record attendance patterns, counselor-related  
2 scheduling and communications, and behavioral signals from which Microsoft generates inferences  
3 about Plaintiffs' and other students' emotions, stress, anxiety, and well-being, as alleged above.

4 54. Under RCW § 19.373.010(8)(b)(xiii), "consumer health data" includes personal  
5 information that identifies a consumer's past, present, or future mental health status, expressly  
6 including information "derived or extrapolated from nonhealth information (such as proxy,  
7 derivative, inferred, or emergent data by any means, including algorithms or machine learning)." Microsoft's inferences about students' emotional states, well-being, anxiety, and mental health—  
8 generated algorithmically from behavioral and telemetric data—are consumer health data within the  
9 statute's express terms, as is the students' self-reported emotional-state data and the medical and  
10 health information contained in their education records.  
11

#### 12 4. Metadata

13 55. Microsoft also collects metadata, which is data that provides contextual information  
14 about the other types of data. For example, student metadata provides contextual information about  
15 student online activity through content and semantic metadata (e.g., the title, author, and subject of  
16 documents and frequency of tool usage, such as grammar suggestions or language translation). It  
17 also provides contextual information about student device use through temporal data (e.g.,  
18 login/logout times and counts, session length, chat timestamps, and assignment-submission times);  
19 network data (e.g., IP addresses, device identifiers, Wi-Fi network IDs, and routing paths); and  
20 device/software data (e.g., OS version, edit history, admin settings, and audit logs).

21 56. Although metadata does not show the exact content students view, it shows the titles,  
22 subjects, structure, timing, and destination of their digital traffic, which it connects to concurrently  
23 collected content and semantic data such that it facilitates profiling even without direct access to the  
24 substantive contents of documents or other materials.

25 ///

26 ///

27 ///

**B. Microsoft uses the many types of student data it obtains to build persistent digital student profiles that are used to influence and predict student behavior.**

**1. Microsoft builds persistent student profiles.**

57. Microsoft continuously aggregates and organizes all the student data it collects, extracts, and generates about students into a digital profile of each student. A student profile is a persistent, centralized, cumulative repository of student data that serves as a unified, evolving digital representation—or blueprint—of the student.

58. These profiles span every aspect of a student’s life, including the following:

- Demographics: who the student is (e.g., age, gender, race)
- Academics: how the student performs (e.g., grades, test scores, attendance)
- Classroom behaviors: how the student interacts with adults and peers (e.g., disciplinary history, participation records, ability to work in groups or independently)
- Digital behaviors: how the student interacts with her device (e.g., browsing history, search logs, app use, online habits)
- Psychology: why the student acts (e.g., triggers, boredom, distraction, mood, vulnerabilities)
- Environment: the student’s context (e.g., location, family, socioeconomics, school, supervision)
- Social behaviors: the child’s relationships (e.g., peer-group clustering, sharing, communications, household information)
- Technical information: details of the student’s device (e.g., firmware version, processing speeds, battery life, admin restrictions)

59. These profiles serve as a longitudinal record of a student’s life that can follow her across classes, school years, devices, websites, apps, and platforms.

60. Microsoft’s profiling is not hypothetical; it is productized and happening now. Microsoft 365 Education includes a suite of analytics features marketed to schools under names including “Education Insights,” which aggregates and displays student-level data on activity, engagement, assignment behavior, and digital habits; “Reading Progress” and “Reading Coach,”

1 which record and algorithmically evaluate students' oral reading, fluency, and errors; "Reflect,"  
2 which collects students' self-reported emotional states; and "Search Coach," which tracks and shapes  
3 students' search behavior within Teams. Each of these features depends on the continuous collection  
4 and algorithmic processing of the student data described above, and each generates derived and  
5 inferred data about individual students that did not previously exist.

## 6 **2. Microsoft's student profiles influence and skew each student's educational** 7 **experience.**

8 61. Microsoft influences and shapes students' educational experiences because it subjects  
9 students to a closed environment in which it continuously collects their data—creating profiles—  
10 and then applies that data to the proprietary algorithms of its internet browser and search engine.  
11 Students with Microsoft accounts, including Plaintiffs, routinely use Microsoft Edge, Microsoft's  
12 browser, and Bing, Microsoft's search engine, for internet searches, including through Microsoft's  
13 "Search Coach" tool built into its Microsoft Teams app.

14 62. Microsoft's internet search algorithms use information specific to an individual user,  
15 including search history, location, and engagement, to deliver unique search results to that user.  
16 Based on Microsoft's documented design of its internet browser and search engine and its collection  
17 of student search and browsing data as alleged herein, these same mechanisms operate on students'  
18 school accounts, delivering results shaped by each student's accumulated profile. Thus, Microsoft  
19 atomizes students' informational environment while enabling Microsoft to extract ever more data  
20 from students as they use the internet.

21 63. Thus, each component of the Microsoft system feeds the next in a never-ending loop.  
22 The students are captives in this system in which Microsoft not only continuously surveils and  
23 datafies them but also decides what content they will view on the internet, all within their compulsory  
24 education and all without their parents' knowledge or consent.

## 25 **3. Microsoft uses student profiles to generate behavioral predictions.**

26 64. Microsoft uses the longitudinal profiles it creates from its continuous data harvesting  
27 to generate digital "tags" about a student in real time. While the content of these tags is virtually

unlimited, some examples include things like, “student’s current scrolling patterns indicate boredom or acute loneliness,” “student exhibits signs of academic anxiety,” or “student is highly triggered by stimulus overload.”

65. Microsoft’s algorithms analyze years of cross-product student tracking and analytics to purportedly identify hidden patterns and assign a risk, behavior, or outcome score to the student. The algorithms then calculate the statistical probability of a future action taken by each student. These “predictions” concern all aspects of a student’s life, such as her academic trajectories, physical and mental well-being, behavioral deviations, and social adaptations.

66. To illustrate how such a system operates: predictive analytics of the kind Microsoft deploys can combine a student’s declining math scores with her history of late logins, counselor visits, and negative sentiment in communications and social-emotional check-ins to generate a score predicting the probability that she will drop out or flagging her as a behavioral risk. Regardless of the accuracy of a particular flag, the student is thereafter understood and treated through the lens of the prediction.

67. This system relies on continuous surveillance and feedback. Raw student data is used to build inferred data, which populates a student profile, which provides context for behavioral predictions, which generate new data points that refine the inferred data, and so on.

68. While the system purports to make predictions that are clearly education-related—e.g., how a student will best absorb and retain information or in what subject she will likely struggle—it also purports to make numerous inferences that are deeply personal and that have only a tenuous connection to education, such as how she spends her free time, what content and communications are likely to upset her, how she feels about her peers, and how she feels about herself. It also purports to determine how the student’s actions, feelings, and behaviors will change under different conditions.

**C. Microsoft’s student profiles create significant risks to students.**

69. Each category of data collected creates a risk to students.

70. For example, metadata enables monitoring even without reviewing content, and it

1 can support conclusions about a student's diligence, responsiveness, isolation, or behavior that may  
2 be inaccurate or unfair.

3 71. Inferred data also poses serious risks to students because it converts their immutable  
4 characteristics and all their behaviors into purportedly actionable, concrete conclusions about the  
5 student. Those conclusions can drive decision-making about a student in countless significant ways.

6 72. Beyond the invasiveness of this practice, the conclusions are entirely resistant to  
7 review, challenge, or correction. Engagement indicators, assignment activity, reading or fluency  
8 measures, collaboration patterns, productivity signals, participation trends, and wellbeing-related  
9 indicators may appear objective because they are generated by software. In reality, the indicators can  
10 be biased by device access, disability, language background, family circumstances, teacher practices,  
11 privacy-protective choices, absenteeism, or inconsistent connectivity. Given that these inferences  
12 drive high-stakes decisions about student intervention, discipline, evaluation, placement, and  
13 resource allocation, students are routinely affected by opaque judgments they cannot see, challenge  
14 or understand.

15 73. While each category of data creates risk, the cumulative risk these categories pose  
16 when combined into a persistent digital profile and used to generate behavioral predictions about  
17 each child is far greater than the sum of those parts.

18 **1. Microsoft generates the equivalent of secret, faulty credit reports for**  
19 **student learning and behavior.**

20 74. The "predictions" Microsoft and others with access to the data make are used in a  
21 host of ways, such as to influence student behavior, to guide decision-making about a student, and  
22 in determining how to allocate school resources. While some uses may inure to a student's benefit,  
23 others do not. For example, a school may decide that a student who is predicted to drop out before  
24 graduation is not worth the school's limited resources. Or a student predicted to behave poorly is  
25 mistreated by school personnel before even engaging in poor behavior.

26 75. Given the opacity and complexity of Microsoft's system, students and parents are left  
27 with no knowledge of important decision-making or recourse to challenge predictions or correct

1 errors. This lack of access and recourse is significant precisely because the system is complex and  
2 ever evolving.

3 76. The system also oversimplifies complex learning behaviors and encourages school  
4 personnel to treat platform activity as a proxy for student effort, comprehension, or character. For  
5 example, an administrator may rely on data and data-derived insights and predictions to identify “at-  
6 risk” students without understanding critical context behind the data.

7 77. As another example, a student who works offline, shares a device with others, has  
8 unreliable internet, avoids chat for privacy reasons, or needs accommodations may be misunderstood  
9 as disengaged or noncompliant.

10 78. Analytics that track clicks, logins, speed, reading fluency, submission timing, or chat  
11 participation may lead to a misinterpretation of accommodated learning as lower performance or  
12 distraction.

13 79. Students who are multilingual, learning English, or communicating in different  
14 dialects may be misclassified by automated language, reading, writing, or fluency tools.

15 80. Platform-derived indicators can penalize students whose families lack stable  
16 broadband, private study space, adult technical support, or flexible schedules. The result is that  
17 poverty-related barriers are reframed as individual student deficits.

18 81. Low chat activity, camera-off participation, delayed logins, missed meetings, or  
19 fewer collaborative edits may reflect anxiety, caregiving responsibilities, shared devices, religious  
20 observance, disability-related needs, transportation issues, or household instability, not  
21 disengagement or defiance.

22 82. Because it is impossible to know the basis of a given conclusion or prediction, the  
23 student will not be properly understood or receive appropriate treatment.

24 83. The numerous risks that flow from a system wholly lacking human-guided contextual  
25 safeguards—and hidden from parents’ review—are not speculative; they are the predictable and real  
26 consequences of the datafication of a student’s life inside Microsoft’s cloud-based education  
27 platform.

1                   **2. Microsoft creates a fractured, exploitative information ecosystem.**

2           84.     These profiles also directly alter a student's online experiences, which are  
3 increasingly serving as students' primary source of information over their teachers or textbooks.

4           85.     Instead of presenting a student with a universal version of the internet, algorithms use  
5 her profile to build a highly customized, reactive online environment. Search results are organized,  
6 not by relevance to search queries, credibility, or educational value, but by what the algorithm  
7 predicts the student will find most engaging based on her profile. The result is a distorted, highly  
8 individualized information ecosystem biased toward an individual student's interests, habits, and  
9 preferences that exploits her vulnerabilities.

10          86.     The risks inherent in this fractured, personalized information ecosystem abound.

11          87.     For example, a student with predicted political leanings may be pushed toward  
12 content that prevents her from exploring other ideas and viewpoints, reinforcing her biases and  
13 polarizing her ideologically.

14          88.     A student who has shown a tendency toward distraction may be served dopamine-  
15 driving, short-form content that leaves him more distracted and less able to exert autonomy over his  
16 attention.

17          89.     A student prone to so-called doomscrolling may be served content that emphasizes  
18 danger, skewing his perception of the world and jeopardizing his mental health.

19          90.     While such content may be facially benign, it becomes harmful when targeted at a  
20 child with a predilection or vulnerability that the content uniquely exploits.

21          91.     Further, in denying students a common informational reality, these systems grossly  
22 compromise the foundational goals of education, including critical thinking, collaboration, and  
23 preparation for civic life.

24       **D. Microsoft continues to engage in excessive and invasive data practices despite legal**  
25       **repercussions.**

26          92.     Microsoft has been found to have collected and used student data without effective  
27 consent through its education products.

1           93. For example, in a 2025 decision, the Austrian Data Protection Authority  
2 (Datenschutzbehörde, “DSB”) found that Microsoft’s deployment of Microsoft 365 Education in  
3 schools involved undisclosed tracking and data practices that neither students nor their guardians  
4 could meaningfully understand or control.<sup>1</sup> The DSB ordered that, as to the minor student  
5 complainant’s Microsoft 365 Education account, Microsoft must provide access to a broad set of  
6 student data—including content (files/documents/messages), system and protocol data (connection  
7 data, log files, IP addresses), cookie data (cookie values), and data transfers to Microsoft—and must  
8 also describe the cookies set or read through Microsoft 365 Education, including whether and how  
9 those cookies resulted in data being transmitted to Microsoft.

10           94. Critically, the DSB treated Microsoft itself as responsible for personal data it received  
11 through Microsoft 365 Education and processed for its own interests, including purposes Microsoft  
12 labeled in vague, abstract terms such as “internal reporting,” “business modeling,” “fraud,”  
13 “cybercrime/cyberattacks,” and “improving core functionality” (including accessibility, privacy, or  
14 energy efficiency)—and ordered Microsoft to provide a concrete, understandable explanation of  
15 what those terms mean in practice, particularly given that the data subject was a child. The DSB also  
16 found that, even by the close of the proceeding, Microsoft had not provided a complete account of  
17 what cookie-related data was processed and on what legal basis, and it highlighted that third parties  
18 such as LinkedIn, ChatGPT/OpenAI, and Xandr appeared in protocol data captured during the  
19 student’s use of Microsoft 365 Education—raising unanswered questions about onward transfers and  
20 recipients.

21           95. Noting that cookie identifiers constitute personal data when linkable to a user  
22 account, the DSB held that non-essential cookies require prior consent; because no such consent  
23 existed, the DSB concluded that the processing of non-essential tracking/telemetry cookies was  
24 unlawful and ordered the responsible parties (including Microsoft) to assess whether data from  
25 specified non-essential cookies was still being processed and, if so, to delete that data.

26  
27 <sup>1</sup>*noyb win: Microsoft 365 Education may not track school children*, noyb (Oct. 10, 2025),  
<https://noyb.eu/en/noyb-win-microsoft-365-education-tracks-school-children>

1           96. In January 2026, the DSB again found that Microsoft was taking student data without  
2 effective consent. It determined that Microsoft was placing tracking cookies on the devices of a  
3 minor student using Microsoft 365 Education. According to Microsoft’s own documentation, these  
4 cookies analyze student behavior, collect student browser data, record session data, and are used for  
5 advertising.<sup>2</sup>

6           97. The DSB further found that Microsoft was the sole party able to reconfigure the  
7 cookie settings. The DSB thus concluded that Microsoft was a “controller” of this data in that it,  
8 alone or jointly with others, determined the purposes and means of processing student data. It found  
9 that Microsoft processes personal data for its own commercial purposes—such as internal reporting,  
10 business modeling, and improving core product functionality—that are inherently in Microsoft’s  
11 interest. It determined that the data Microsoft collected was not technically necessary.

12           98. The DSB observed that consent was required even if the data had been  
13 pseudonymized. It found that Microsoft had not obtained consent or made any attempt to obtain  
14 consent.

15           99. Beyond the educational context, other nations have found Microsoft failing to inform  
16 its users of how much personal data it collects about them. In 2018–2019, the Dutch Ministry of  
17 Justice and Security (“DMJS”) found that a Microsoft product collected extensive telemetry data,  
18 including metadata and potentially sensitive interactions. DMJS concluded that Microsoft was  
19 processing personal data—including content that could be linked back to specific users or  
20 identifiable devices—without sufficient transparency or user control and declared Microsoft’s  
21 practices in violation of EU data protection laws.

22           100. In July 2022, the French data protection authority, the Commission nationale de  
23 l’informatique et des libertés (“CNIL”), determined that Microsoft failed to obtain valid consent  
24 before placing tracking cookies for advertising and telemetry purposes in its Windows and Microsoft  
25 365 services, that the data collection enabled the company to profile users’ behavior across services,  
26

---

27 <sup>2</sup>*noyb win: Microsoft ordered to stop tracking school children*, noyb (Jan. 27, 2026),  
<https://noyb.eu/en/noyb-win-microsoft-ordered-stop-tracking-school-children>

1 and that the telemetry allowed re-identification of individuals. CNIL imposed a €60 million fine on  
2 Microsoft for violating the GDPR's transparency and consent requirements.

3 101. The United States government has also taken action against Microsoft for its  
4 nonconsensual data collection practices involving children. In 2023, the FTC settled a suit it brought  
5 against Microsoft for \$20 million based on Microsoft's multiple alleged violations of COPPA (1) by  
6 collecting personal information from children under 13 before notifying their parents and obtaining  
7 parental consent; (2) by failing to tell parents about the information the company collects from  
8 children, why it is collecting that information, and the fact that it discloses some of the data to third  
9 parties; and (3) by retaining children's personal information for longer than is reasonably necessary.

10 102. Despite these legal repercussions and reprimands, Microsoft continues to engage in  
11 excessive data collection and profiling in schools beyond any permissible educational interest and  
12 without effective consent.

13 **E. Microsoft exploits student data for its own commercial purposes.**

14 103. Microsoft uses student data, including Plaintiffs' data, for commercial purposes,  
15 including, among other things, to advertise and promote its Products, to train artificial-intelligence  
16 models, and to improve and develop its Products and business.

17 104. Microsoft is required by law to obtain parental consent before engaging in any of  
18 these activities, and neither Plaintiffs nor their parents consented to Microsoft using their personal  
19 information in these ways.

20 105. Data flows freely between various Microsoft products in a system designed to  
21 continuously collect, analyze, and use students' and other users' personal information.

22 106. Fueled by its ever-growing trove of personal information, including Plaintiffs'  
23 personal information, Microsoft's suite of cloud-based online products now includes dozens of data-  
24 extracting and data-derived products.

25 107. The personal information collected from students, including Plaintiffs, through  
26 Microsoft's Products is not segregated, and the collection and use of that personal information is not  
27 limited to the platforms and products licensed by schools.

108. Microsoft uses the profiles it creates about students for data analytics—identifying patterns, trends, and insights—about almost every area of a student’s life. This allows Microsoft to understand and analyze children’s behaviors, interests, habits, purchasing preferences, academic performance, and more; build, develop, and market products accordingly; and then predict how the children will operate in the future for use in its own commercial planning, projections, targeted marketing, and other targeted content provision, which all allow Microsoft to grow its revenue.

109. Further, one of the technologies Microsoft developed and continues to develop using students’ personal data, including Plaintiffs’ data, is its AI technology, which Microsoft has incorporated and continues to incorporate into its suite of products.

110. Microsoft calls its standard AI technology “Copilot” and has integrated it into at least 80 of its products.<sup>3</sup>

111. Microsoft has also partnered with OpenAI (an AI research and deployment company known for creating advanced AI models such as ChatGPT and DALL-E) since 2019. In October 2025, Microsoft announced that it “signed a new definitive agreement” with OpenAI, part of which includes Microsoft investing approximately \$135 billion with OpenAI Group PBC, which is the for-profit corporate entity of OpenAI.<sup>4</sup> In November 2025, it announced that it was also expanding its existing partnership with Anthropic, the other largest private AI company.<sup>5</sup> It announced that it would expand its integration of Anthropic’s AI model within its products and invest up to \$5 billion in the company.<sup>6</sup>

112. Microsoft is committed to growing AI capabilities as much as possible and has stated, “We envision a world in which agents operate across individual, organizational, team and end-to-

---

<sup>3</sup> *How many products does Microsoft have named ‘Copilot’?? I mapped every one*, Tey Bannerman (March 31, 2026), <https://teybannerman.com/strategy/2026/03/31/how-many-microsoft-copilot-are-there.html>

<sup>4</sup> *Our structure*, OpenAI, <https://openai.com/our-structure/> (last visited Aug. 1, 2026); *Built to benefit everyone*, OpenAI (Oct. 28, 2025), <https://openai.com/index/built-to-benefit-everyone/>

<sup>5</sup> *Microsoft, NVIDIA and Anthropic announce strategic partnerships*, Microsoft (Nov. 18, 2025), <https://blogs.microsoft.com/blog/2025/11/18/microsoft-nvidia-and-anthropic-announce-strategic-partnerships/>

<sup>6</sup> *Id.*

1 end business contexts. This emerging vision of the internet is an open agentic web, where AI agents  
2 make decisions and perform tasks on behalf of users or organizations.”<sup>7</sup>

3 113. After renegotiating its agreement with OpenAI to allow it to explore its own AI  
4 research, Microsoft has now also been deploying several of its own AI models in many of its products  
5 and plans to substantially expand its own AI models and capabilities.<sup>8</sup> In June 2026, the CEO of  
6 Microsoft AI stated: “Our job is to make sure that when we look out to 2030 and beyond, we have  
7 the capacity not just to buy models from third parties, but to build the absolute frontier, the best  
8 models in the world.”<sup>9</sup>

9 114. Microsoft claims that student data is collected only for educational purposes and is  
10 not exploited for Microsoft’s own purposes, including its AI development. Microsoft further claims,  
11 in substance, that data belonging to its education customers remains isolated within their own cloud  
12 environments and is not used to train its foundation AI models. A “tenant” is Microsoft’s term for  
13 the walled-off instance of its cloud services provisioned to each customer organization—here, each  
14 school district’s own container of student accounts, files, and administrative controls within  
15 Microsoft 365 Education. Microsoft’s claims, however framed, extend at most to the content held  
16 within a school district’s tenant.

17 115. In fact, on information and belief, based on the design and mechanics of the Products,  
18 Microsoft’s own documentation of its telemetry and required service data practices, and the findings  
19 of the Austrian Data Protection Authority described above, Microsoft collects telemetry, diagnostic,  
20 usage, and engagement data generated by students that flows outside the boundaries of school  
21 tenants—beyond schools’ visibility and control and contrary to Microsoft’s claims that student data

---

22 <sup>7</sup> *Microsoft Build 2025: The age of AI agents and building the open agentic web*, Microsoft (May  
23 19, 2025), [https://blogs.microsoft.com/blog/2025/05/19/microsoft-build-2025-the-age-of-ai-agents-](https://blogs.microsoft.com/blog/2025/05/19/microsoft-build-2025-the-age-of-ai-agents-and-building-the-open-agentic-web/)  
24 [and-building-the-open-agentic-web/](https://blogs.microsoft.com/blog/2025/05/19/microsoft-build-2025-the-age-of-ai-agents-and-building-the-open-agentic-web/)

25 <sup>8</sup> *Microsoft Build 2026: Be yourself at work*, Microsoft (June 2, 2026),  
<https://blogs.microsoft.com/blog/2026/06/02/microsoft-build-2026-be-yourself-at-work/>

26 <sup>9</sup> Michael Nuñez, *Microsoft AI chief says company was “set free” from OpenAI to pursue*  
27 *superintelligence* (June 5, 2026), [https://venturebeat.com/technology/microsoft-ai-chief-says-](https://venturebeat.com/technology/microsoft-ai-chief-says-company-was-set-free-from-openai-to-pursue-superintelligence)  
[company-was-set-free-from-openai-to-pursue-superintelligence](https://venturebeat.com/technology/microsoft-ai-chief-says-company-was-set-free-from-openai-to-pursue-superintelligence)

1 remains isolated within the tenant—and uses that data for its own purposes, including analytics,  
2 product development, and the training, testing, tuning, and improvement of its algorithms and AI-  
3 enabled features. That data originates with, describes, and is extracted from students, whatever label  
4 Microsoft assigns it.

5 116. Neither Plaintiffs nor their parents consented to Microsoft using their personal  
6 information in this manner.

7 117. Although Microsoft purports to confer administrative and pedagogical benefits to  
8 schools and school districts through its Products, these Products are undeniably commercial, for-  
9 profit Products that integrate deeply with Microsoft’s data-driven cloud infrastructure and analytics  
10 systems, enabling Microsoft to derive significant commercial value from student data in ways that  
11 compromise student privacy and far exceed what parents, students, and schools reasonably expect  
12 and what is reasonably necessary for legitimate educational purposes.

13 **F. Plaintiffs extensively use Microsoft’s Products for school.**

14 118. Plaintiffs incorporate all preceding paragraphs by reference, as Plaintiffs and all other  
15 students using Microsoft’s Products for school are subject to the same data practices.

16 119. Plaintiffs are required to use Microsoft’s Products at their schools. A.W. and M.W.  
17 use all the Products, including Microsoft Edge, Microsoft Windows 10 and Windows 11, Microsoft  
18 365 Education, and Minecraft Education. H.W.1 and H.W.2 use Microsoft Edge, Microsoft Windows  
19 11, and Minecraft Education.

20 120. The school created the Microsoft Edge, Microsoft Windows 10, Windows 11,  
21 Microsoft 365 Education, and Minecraft Education accounts for Plaintiffs, and their parents were  
22 not provided with any terms or policies pertaining to the Products, nor were they given an  
23 opportunity to provide or withhold consent to Microsoft’s data practices. Neither Plaintiffs nor their  
24 parents consented to Microsoft’s generation or collection of Plaintiffs’ personal information through  
25 their use of the Products.

26 121. The data submitted by Plaintiffs through Microsoft Edge, Microsoft Windows 10,  
27 Microsoft Windows 11, Microsoft 365 Education, and Minecraft Education is highly personal: it

1 facilitates insights and predictions regarding their skill mastery, habits, interests, academic strengths  
2  
3 and weaknesses, development, psychology, social behavior, overall well-being, family life, and  
4 vulnerabilities.

5 122. Microsoft has thus collected and generated—and continues to collect and generate—  
6 vast troves of personal data belonging to Plaintiffs, including their personal information, through  
7 their use of its Products. And Microsoft uses the collected and generated data to continuously create  
8 and add to evolving, robust, highly detailed personal and sensitive profiles on Plaintiffs that are used  
9 for Microsoft’s commercial benefit.

10 123. Ms. Williams requested access from Microsoft to the personal data it has collected  
11 about each of her four children. Microsoft failed to comply with her requests as to any of them. As  
12 to H.W.1 and H.W.2, who are under 13, Microsoft’s refusal deprived Ms. Williams of her right under  
13 COPPA to know, review, or correct the information Microsoft holds about her children, and confirms  
14 that parents cannot discover Microsoft’s practices through reasonable diligence.

15 **1. Plaintiffs’ use of Microsoft Edge.**

16 124. Plaintiff A.W. uses Microsoft Edge at his school. He began using Microsoft Edge in  
17 or about September 2015 shortly after he began his education in the Spokane Public Schools. He  
18 was six years old. A.W. regularly used Microsoft Edge and its default search engine, Bing, from  
19 2015 to 2026 to browse the internet and access the Word, Excel, PowerPoint, Teams, and Outlook  
20 applications in Microsoft 365 Education. He currently uses Microsoft Edge at school for a minimum  
21 of 30 minutes per day.

22 125. Plaintiff M.W. also uses Microsoft Edge at his school. He began using Microsoft Edge  
23 in or about September 2018 when he began his education in the Spokane Public Schools. He was 5  
24 years old. M.W. regularly used Microsoft Edge and its default search engine, Bing, starting in 2018  
25 and continuing to the present day, to browse the internet and access Microsoft 365 Education  
26 applications, including Word, Excel, PowerPoint, Teams, and Outlook. He currently uses Microsoft  
27 Edge at school for a minimum of 30 minutes per day.

1           126. Plaintiff H.W.1 began his education in the Spokane Public Schools in September  
2 2020 when he was five years old. His school district requires that he use the Microsoft Edge web  
3 browser as part of his schooling and has required that he do so since he began school.

4           127. Plaintiff H.W.2 began his education in the Spokane Public Schools in September 2024  
5 when he was five years old. His school district requires that he use the Microsoft Edge web browser  
6 and has required that he do so since he began school.

7           128. Prior to 2025, Plaintiffs were permitted to bring their school-assigned Microsoft  
8 laptops home to complete and submit homework assignments. From approximately 2020 to 2024,  
9 Plaintiffs regularly submitted homework via Microsoft Edge. Beginning in 2025, Plaintiffs have not  
10 been permitted to bring their laptops home, but they still regularly access Microsoft Edge to complete  
11 required schoolwork for a minimum of 30 minutes per day.

## 12                   **2. Plaintiffs' use of Windows 10 and Windows 11.**

13           129. Plaintiff A.W. has used Windows 10 and Windows 11 at his schools. At the beginning  
14 of each school year since he began school in the Spokane Public Schools, Plaintiff A.W. was  
15 provided with a laptop operating on Windows 10, and later, Windows 11, for use for school. Plaintiff  
16 A.W. regularly used Windows 10 each year to log into his school account and access applications,  
17 files, and online resources, until he was instead required to use Windows 11. Since switching to  
18 Windows 11, Plaintiff A.W. regularly used Windows 11 each year to log into his school account and  
19 access applications, files, and online resources.

20           130. Plaintiffs M.W., H.W.1 and H.W.2 have used Windows 11 at their schools. At the  
21 beginning of each school year since they began school in the Spokane Public Schools, Plaintiffs  
22 M.W., H.W.1 and H.W.2 were each provided with a device operating on Windows 11 for use for  
23 school. Plaintiffs M.W., H.W.1 and H.W.2 regularly used Windows 11 each year to log into their  
24 school accounts and access applications, files, and online resources.

25           131. Plaintiffs A.W., M.W., H.W.1, and H.W.2 currently use Windows 11 daily to complete  
26 required tasks for school.  
27

1                   **3. Plaintiffs' use of Minecraft Education.**

2           132. Plaintiff A.W. used Minecraft Education on a school-issued computer from 2014 to  
3 2019 while in the Spokane Public Schools system. He used Minecraft Education for approximately  
4 12 hours per week for the 2014-2015 school year, approximately 10 hours per week for the 2015-  
5 2016 school year, approximately 5 hours per week for the 2016-2017 school year, and approximately  
6 2 hours per week for the 2018-2019 school year.

7           133. Plaintiff M.W. used Minecraft Education on a school-issued computer from 2018 to  
8 2024 while in the Spokane Public Schools system. He used Minecraft Education for approximately  
9 15 hours per week for the 2018-2019 school year, approximately 10 hours per week for the 2019-  
10 2020 school year, approximately 10 hours per week for the 2020-2021 school year, approximately  
11 10 hours per week for the 2021-2022 school year, approximately 10 hours per week for the 2022-  
12 2023 school year, and approximately 10 hours per week for the 2023-2024 school year.

13           134. Plaintiff H.W.1 used Minecraft Education on a school-issued computer from 2020 to  
14 2025, while in the Spokane Public Schools system. He used Minecraft Education for approximately  
15 15 hours per week for the 2021-2022 school year, approximately 12 hours per week for the 2022-  
16 2023 school year, approximately 10 hours per week for the 2023-2024 school year, and  
17 approximately 10 hours per week for the 2024-2025 school year.

18           135. Plaintiff H.W.2 used Minecraft Education on a school-issued computer from 2024 to  
19 2026, while in the Spokane Public Schools system. He used Minecraft Education for approximately  
20 10 hours per week for the 2024-2025 school year, and approximately 10 hours per week for the  
21 2025-2026 school year.

22                   **4. A.W.'s and M.W.'s use of Microsoft 365 Education.**

23           136. Plaintiff A.W. uses Microsoft 365 Education at his school. He began using Microsoft  
24 365 Education in or about 2021 when he entered middle school in the Spokane Public Schools. He  
25 was 11 years old. A.W. regularly used Microsoft 365 Education to complete assignments, create  
26 content, send and receive online communications, conduct research, and take notes. Within  
27 Microsoft 365 Education, A.W. accessed and used several Microsoft applications, including Word,

Excel, PowerPoint, Teams and Outlook. He currently uses Microsoft 365 Education daily.

137. Plaintiff M.W. also uses Microsoft 365 Education at his school. He began using Microsoft 365 Education in or about 2024 when he entered middle school in the Spokane Public Schools. He was 11 years old. M.W. regularly used Microsoft 365 Education to complete assignments, create content, send and receive online communications, conduct research, and take notes. Within Microsoft 365 Education, M.W. accessed and used several Microsoft applications, including Word, Excel, PowerPoint, Teams and Outlook. He currently uses Microsoft 365 Education daily at school.

**G. Microsoft's data practices harm students.**

138. Microsoft's surreptitious data practices are not benign. Rather, they harm and create significant risks for children, including Plaintiffs, in myriad ways that are immediate, long-lasting, and substantial.

**1. Microsoft harms children, including Plaintiffs, by invading their privacy.**

139. A person's right to privacy begins with protection from having information created about him or her in the first instance.

140. 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.

141. Microsoft's data practices violate Plaintiffs' and other children's fundamental right to privacy, a legally protected interest. They 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.

142. Microsoft collects and uses personal information about school-aged children for its own commercial benefit from data it takes from students while they use its Products as part of their legally required education.

///

///

1           143. The types and amount of personal student information Microsoft collects, generates,  
2 and uses far exceed what could be considered reasonable for legitimate educational interests or  
3 purposes.

4           144. Microsoft also uses student data to build highly detailed and dynamic psychographic  
5 profiles of students used to predict and influence their behavior. Such intimate surveillance and  
6 profiling are inherently antithetical to a child's right to privacy.

7           145. That Microsoft targets minors in a compulsory environment and without parental  
8 notice or consent is conduct that is highly offensive to a reasonable person and constitutes an  
9 egregious breach of social norms.

10           146. The privacy harm to Plaintiffs and other Washington schoolchildren occurred at the  
11 first moment Microsoft began taking their personal information without effective consent and is  
12 ongoing as long as Microsoft continues to do so.

13                   **2. Microsoft harms children by failing to compensate them for their**  
14                   **involuntary labor.**

15           147. In addition to invading students' privacy, Microsoft also forces students—who are  
16 required to use its Products as part of their compulsory education—to serve as perpetual test and  
17 data subjects, providing real-world information about the usability and functionality of its Products,  
18 helping it understand how well its search algorithms engage different groups of children, and  
19 providing real-world information about the trends, patterns, interests and preferences of children in  
20 their demographics.

21           148. Companies routinely compensate members of their target user base or others to serve  
22 as test or data subjects for these reasons. For example, Google offers rewards in the form of gift  
23 cards for consumers who agree to enroll their smartphone devices to share website and app activity  
24 data with Google.<sup>10</sup> Google states that the purpose of the study is “to understand the combined data  
25 of all participants so that Google can develop products that improve the experience for all users.”<sup>11</sup>

26           

---

<sup>10</sup> *Device Usage Study*, Google, <https://deviceusagestudy.google/signup/invitecode> (last visited Aug.  
27 1, 2026).

<sup>11</sup>*Id.*

149. Microsoft itself offers a rewards program in which consumers can register with Microsoft and earn rewards when they conduct their internet searches through Bing on their PCs or mobile devices or begin searches in their Windows search boxes. Microsoft states that the participants can earn “gift cards, sweepstakes entries, nonprofit donations, and more.”<sup>12</sup>

150. Tellingly, Microsoft requires parental consent before children under 13 can participate in its Rewards program, as is required by COPPA.<sup>13</sup> And Microsoft has a procedure for obtaining parental consent for the program.<sup>14</sup> Yet, Microsoft persists in failing to obtain parental consent when it takes all of the same data and far more from students who are required to use its products in schools.

151. The telemetry and behavioral tracking that Microsoft conducts on students as they engage in their required schoolwork allows Microsoft to understand data such as how long it takes students to compose an email or how often students click on certain tools or websites, which then allows it to redesign its interfaces without the necessity of obtaining direct user feedback.

152. This is also true for Microsoft’s design of its algorithms, as analysis of the types of content that increases student engagement or keeps them on the platform longer can allow Microsoft to tweak its algorithms, test again, and keep refining them to maximize overall user engagement and time on the platform.

153. Thus, Microsoft takes advantage of Plaintiffs’ and other students’ required use of its Products to use the students as unpaid data and test subjects so that Microsoft can grow its business and increase its revenue, all without providing notice of its practices to their parents or obtaining parental consent.

154. Microsoft’s actions have thus caused Plaintiffs and putative class members economic

---

<sup>12</sup>*Microsoft Rewards*, Microsoft, <https://rewards.bing.com/welcome#areaheading-uid7624> (last visited Aug. 1, 2026).

<sup>13</sup>*Learn about Microsoft Rewards*, Microsoft, <https://support.microsoft.com/en-US/accounts-billing/rewards/learn-about-microsoft-rewards> (last visited Aug. 1, 2026).

<sup>14</sup>*Managing Parental Consent*, Microsoft, <https://support.microsoft.com/en-US/family-safety/managing-parental-consent> (last visited Aug. 1, 2026).

injury because Plaintiffs' and other students' labor would otherwise be entitled to compensation if not for Microsoft's wrongful conduct.

**3. Microsoft harms children by failing to compensate them for and diminishing the value of their property.**

155. Washington courts recognize that personal information has value, and Washington laws demonstrate a public policy recognizing value in the security of one's personal information.

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

157. Microsoft itself recognizes that personal data has value, as evidenced by its Rewards program discussed above showing that it compensates consumers for using its search tools.

158. Student data is valuable because it can be used to develop, deliver, and improve products and services; personalize and target marketing; identify and manage risk; and predict future behaviors and trends.<sup>15</sup> Younger data subjects mean more years over a lifetime for corporations to track and use data for targeted advertising and other commercial purposes and thus maximize profits.

159. By generating, collecting, and monetizing student information, education technology, or "EdTech,"<sup>16</sup> has become a more than \$200 billion global industry that is projected to more than double by 2034.<sup>17</sup> Investors have taken note. Investments in EdTech surged from \$500 million in 2010 to \$16.1 billion in 2021.<sup>18</sup>

---

<sup>15</sup>Hamed Ghorban Tanhaei, *Predictive analytics in customer behavior: Anticipating trends and preferences* (2024), <https://www.sciencedirect.com/science/article/pii/S2666720724000924>.

<sup>16</sup> 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).

<sup>17</sup>*EdTech Market Overview*, Fortune Business Insights, <https://www.fortunebusinessinsights.com/edtech-market-111377> (last updated July 13, 2026).

<sup>18</sup>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>.

1           160. Even back in 2014, when EdTech funding was at \$1.87 billion,<sup>19</sup> a leading EdTech  
2 executive described education as “the world’s most data-mineable industry by far” and stated that  
3 “[w]e literally know everything about what you know and how you learn best, everything.”<sup>20</sup> The  
4 EdTech industry’s presence in schools has become far more prevalent since then. As one leading  
5 EdTech investor explained, the investments in EdTech are not philanthropic: the purpose of these  
6 private EdTech ventures “isn’t a social mission . . . . They’re there to create return.”<sup>21</sup>

7           161. Most U.S. consumers value their data and their privacy. Accordingly, an  
8 overwhelming majority engage in efforts to protect their data: 86 percent of U.S. consumers report  
9 caring about data privacy and wanting more control; 79 percent are willing to spend time and money  
10 to protect their data; and nearly half have terminated relationships with both online and traditional  
11 companies over data-privacy concerns, especially younger consumers.

12           162. Nearly 90 percent of U.S. online adults use at least one privacy- or security-protecting  
13 tool online.

14           163. The information Microsoft collects has significant economic value.

15           164. Microsoft’s own conduct establishes the market price of the data at issue. Through its  
16 Rewards program, Microsoft pays consumers—in gift cards, sweepstakes entries, and charitable  
17 donations—for the very categories of data it takes from students without payment: search queries,  
18 browsing behavior, and engagement signals generated through Bing and Windows search. Microsoft  
19 sets and publishes the exchange rate itself.

20 ///

---

21  
22  
23 <sup>19</sup> CBInsights, *EdTech Funding Hits \$1.87 Billion in 2014*, [https://www.cbinsights.com/research/ed-](https://www.cbinsights.com/research/ed-tech-funding-record-2014/)  
24 [tech-funding-record-2014/](https://www.cbinsights.com/research/ed-tech-funding-record-2014/) (Jan. 20, 2025).

25 <sup>20</sup>Stephanie Simon, *The big biz of spying on little kids*, Politico (May 15, 2014),  
26 <https://www.politico.com/story/2014/05/data-mining-your-children-106676>; Adriene Hill, *A day in*  
*the life of a data mined kid*, Marketplace (Sept. 15, 2014), [https://www.marketplace.org/](https://www.marketplace.org/story/2014/09/15/day-life-data-mined-kid)  
[story/2014/09/15/day-life-data-mined-kid](https://www.marketplace.org/story/2014/09/15/day-life-data-mined-kid)

27 <sup>21</sup> *Id.*

1           165. Microsoft thus assigns a concrete, quantifiable per-user, per-search value to this data  
2 when it must bargain for it. When Microsoft takes identical—and more extensive—data from captive  
3 students, it simply keeps that value for itself. The value Microsoft pays willing participants through  
4 its Rewards program is a floor, not a ceiling, on the value of the data taken from Plaintiffs and Class  
5 members, because student data is more valuable: it is longitudinal, begins earlier in life, spans more  
6 contexts, and includes categories (behavioral, telemetric, social-emotional, and inferred data) that  
7 Rewards participants do not surrender.

8           166. Plaintiffs and Class members were deprived of this value. Had Microsoft not taken  
9 their data without consent, Plaintiffs and Class members would have retained the ability to withhold  
10 it, to bargain for its value as Rewards participants do, or to decline any exchange at all.

11           167. Microsoft profits from students by acquiring their sensitive and valuable personal  
12 information—which includes far more than mere demographic information perhaps necessary for  
13 obtaining consent such as name, birth date, and contact information—by using the information to  
14 build, develop, improve, and market its Products.

15           168. These practices circumvent students' efforts to prevent others from accessing their  
16 data.

17           169. Microsoft's actions have thus caused Plaintiffs and putative class members economic  
18 injury.

19           170. By collecting, using, and disclosing Plaintiffs' information, Microsoft diminished the  
20 value of that information and Plaintiffs' current and future property interest in it.

21           171. In exchange for Microsoft's collection and use of Plaintiffs' information, all Plaintiffs  
22 received was the ability to exercise their fundamental right to an education to which they were already  
23 entitled.

24           172. By taking Plaintiffs' personal data without their knowledge or consent and without  
25 compensating them, Microsoft forced Plaintiffs to participate in a transaction in which they gained  
26 less than they otherwise would have gained had they been given a choice, including the choice not to  
27 enter into the transaction.

173. Microsoft's actions caused damage to and loss of Plaintiffs' right to control the collection, dissemination, and use of their personal information.

174. The harms to Plaintiffs' personal property occurred the moment Microsoft first began collecting the information and using it for its commercial benefit. The harms continue at least until Microsoft ceases to engage in the wrongful conduct alleged herein.

**4. Microsoft harms children, including Plaintiffs, by compromising the security of their personal information.**

175. Microsoft does not store students' sensitive information in a single, locked-down vault on school grounds that is accessible only to school personnel. Instead, it relies on a cloud infrastructure that necessarily requires multiple parties to access, process, and interact with the data to keep the systems running and secure.

176. Thus, by collecting, retaining, and storing children's personal information, including Plaintiffs' personal information—and by creating information about them that did not previously exist, such as digital profiles that aggregate students' academic, behavioral, and social-emotional data—Microsoft engages in an affirmative act creating a high degree of risk that the information will be stolen, compromised, misused, lost, or retained long after the purported educational purpose has ended. Further, Microsoft's acts *forever* jeopardize the information, as Microsoft uses broad access controls, inadequately governs its exports, shares the information with vendors under opaque and ever-changing agreements, and continues storing it indefinitely.

177. In addition, Microsoft's collection of student behavioral data poses unique risks to students because such data reveals highly sensitive information about a student's interests, habits, and intentions, which are vulnerable to exploitation. Even if such data does not explicitly identify a student, it may be readily reidentified.

178. Metadata may be the highest-risk category precisely because it can seem less sensitive than other types of data and be less protected even though it is the connective tissue between the other types of data. It maps relationships, routines, and participation. It reveals an enormous amount of information about a student's routines, relationships, pace of work, attendance patterns,

1 social connections, and classroom engagement.

2 179. Further, rates of cybercrime are steadily rising, and education is a high-priority target.  
3 Schools and school districts have been particularly and increasingly targeted by cybercriminals in  
4 recent years, resulting in leaks of highly personal information about children that was sometimes  
5 even made publicly available.

6 180. For example, one widely used EdTech company was hacked twice within a two-week  
7 span in May 2026. A criminal-extortion group took credit and, after the first hack, threatened that if  
8 the company did not pay a ransom, the group would leak “[s]everal billion . . . private messages  
9 among students and teachers and students and other students involved, containing personal  
10 conversations and other [personally identifiable information].”<sup>22</sup> The EdTech company  
11 acknowledged in a public statement that the stolen data included identifying information “such as  
12 names, email addresses, and student ID numbers, as well as messages among users.”<sup>23</sup>

13 181. When the company did not cooperate with the criminal group, the group hacked it a  
14 second time, obtaining more data and disrupting teachers’ and students’ access to the company’s  
15 services in schools throughout the country.<sup>24</sup> The company then announced that it “reached an  
16 agreement with the unauthorized actor involved in th[e] incident” and claimed that the data was  
17 returned and destroyed and that the criminal group claimed it would not extort individual  
18 customers.<sup>25</sup>

19 182. When companies pay ransoms to hackers, it encourages more hackers to follow suit.  
20 Indeed, the FBI “does not support paying a ransom” because it “doesn’t guarantee you . . . will get  
21 any data back” and “encourages perpetrators to target more victims and offers an incentive for others  
22

---

23 <sup>22</sup>“PAY OR LEAK”: Hackers Target Big Higher Ed Vendor, Inside Higher Tech (May 5, 2026),  
24 <https://www.insidehighered.com/news/tech-innovation/administrative-tech/2026/05/05/pay-or-leak-hackers-target-big-higher-ed-vendor>

25 <sup>23</sup>Confirmed Security Incident, Instructure, <https://status.instructure.com/> (visited Apr. 29, 2026).

26 <sup>24</sup>Hanna Park, Ramishah Maruf, Emma Tucker, *What we know about the Canvas hack that has*  
27 *impacted thousands of schools*, CNN (May 8, 2026), <https://www.cnn.com/2026/05/07/us/canvas-hack-strands-college-students-finals-week>

<sup>25</sup>Security Incident Update & FAQs, Instructure, [https://www.instructure.com/incident\\_update](https://www.instructure.com/incident_update)  
(visited May 14, 2025).

1 to get involved in [it].”<sup>26</sup>

2 183. The same criminal group involved in the May 2026 attacks also hacked another  
3 EdTech company only two months before that, in March 2026.<sup>27</sup> The company acknowledged the  
4 breach and ransom demand but claimed the stolen data was that of school staff members and not  
5 students.<sup>28</sup> Yet another EdTech company was hacked and subject to a ransom demand in  
6 December 2024, compromising the personal information of tens of millions of students dating back  
7 four decades.<sup>29</sup> The hacker in that case was a college student who stated after his arrest that “it’s  
8 easy, easy money” and that he was “thankful for [the FBI] . . . because [he] would have never  
9 stopped.”<sup>30</sup>

10 184. Educational data is also a high-priority target for nation-state threat actors.  
11 Microsoft’s own 2024 Digital Defense Report found that the education and research sector was the  
12 second-most targeted sector by nation-state threat actors from Russia, China, Iran, and North  
13 Korea.<sup>31</sup>

14 185. Such exposure can have immediate and long-term consequences for children. As  
15 explained by one cybersecurity professional whose son’s school was hacked, “It’s your future. It’s  
16  
17

---

18 <sup>26</sup>*How We Can Help You*, FBI.gov, [https://www.fbi.gov/how-we-can-help-you/scams-and-](https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware)  
19 [safety/common-frauds-and-scams/ransomware](https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware) (last visited Aug. 1, 2026).

20 <sup>27</sup>*School software serving 11M students hacked, ShinyHunters claims attack*, cybernews,  
21 <https://cybernews.com/security/software-11m-students-hacked-shinyhunters-attack/> (last visited  
22 Aug. 1, 2026).

23 <sup>28</sup>*Notice regarding a security incident*, Infinite Campus (Mar. 22, 2026),  
24 [https://content.govdelivery.com/attachments/NCSBE/2026/03/23/file\\_attachments/3591917/Infinite](https://content.govdelivery.com/attachments/NCSBE/2026/03/23/file_attachments/3591917/InfiniteCampusMarch22_note.PNG.pdf)  
25 [eCampusMarch22\\_note.PNG.pdf](https://content.govdelivery.com/attachments/NCSBE/2026/03/23/file_attachments/3591917/InfiniteCampusMarch22_note.PNG.pdf)

26 <sup>29</sup>*Malware stole internal PowerSchool passwords from engineer’s hacked computer*, TechCrunch  
27 (Jan. 17, 2025), [https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-](https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-passwords-from-engineers-hacked-computer/)  
28 [passwords-from-engineers-hacked-computer/](https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-passwords-from-engineers-hacked-computer/)

29 <sup>30</sup>*College student who hacked PowerSchool software says he’s grateful he was caught*, WMRU9abc  
30 (Apr. 16, 2026), [https://www.wmur.com/article/college-student-hack-powerschool-](https://www.wmur.com/article/college-student-hack-powerschool-41426/71017881)  
31 [41426/71017881](https://www.wmur.com/article/college-student-hack-powerschool-41426/71017881)

32 <sup>31</sup>*Microsoft Digital Defense Report 2024*, Microsoft, [https://www.microsoft.com/en-](https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024)  
33 [us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024](https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024) (last visited  
34 Aug. 1, 2026).

1 getting into college, getting a job. It's everything."<sup>32</sup> Regarding the 2024 EdTech data breach, a  
2 former FBI official said that "[i]t was one of the worst I've seen here when you talk about financial  
3 impact. You talk about the forever impact that these students and faculty will have for the rest of  
4 their lives."<sup>33</sup>

5 186. Microsoft's sweeping, invasive, and indiscriminate data practices unduly  
6 compromise the security of children's personal and private information and create a risk that their  
7 misappropriated personal information will be misused in the future, causing them further privacy  
8 and economic harms.

9 187. In sum, Microsoft's data practices harm children from the moment their personal  
10 information is generated or otherwise obtained by Microsoft.

11 188. That harm is exacerbated by Microsoft's persistent storage, use, and disclosure of that  
12 information to third-party vendors.

13 189. The security harms to Plaintiffs and other Washington schoolchildren occurred when  
14 Microsoft began collecting, retaining, storing, generating, and sharing their personal information  
15 without notice to their parents and without effective consent, and the harms continue as long as  
16 Microsoft persists in its wrongful conduct.

17 **H. Microsoft's persistent practice of nonconsensual surveillance, data mining, predictive**  
18 **profiling, and profiteering is unfair, unjust, and violates students' rights.**

19 190. Schools have always been authorized to collect and use certain student information  
20 to provide education services and a safe learning environment, and in modern-day education, often  
21 engage EdTech companies to do so. But there are limits to the types and amount of student  
22 information that may be collected and used without first obtaining parental consent. The limits are

---

23  
24 <sup>32</sup> Natasha Singer, *A Cyberattack Illuminates the Shaky State of Student Privacy*, The New York  
25 Times (July 31, 2022), <https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html>

26 <sup>33</sup> "I was addicted to hacking": Teen tells how gaming led to cybercrime, breaching nationwide  
27 school systems, including Texas, WFAA ABC News (May 1, 2026),  
<https://www.wfaa.com/article/news/crime/teen-tells-how-gaming-led-to-cybercrime-breaching-nationwide-school-systems-including-texas/287-1fcef3dc-f067-4de4-8c06-10bac85ce180>

1 set and informed by state and federal laws that protect the privacy of students and minors and parents'  
2 rights over their children's information.

3 191. Defining the permissible boundaries of mandatory student data practices is a highly  
4 fact-intensive undertaking and one that necessarily changes with time and technological  
5 developments. The massive surveillance and data-extraction apparatus deployed in K-12 education  
6 by Microsoft far exceeds those boundaries, and Microsoft collects, generates, and uses far more  
7 personal student data than what could be reasonably expected or necessary for legitimate educational  
8 interests or purposes.

9 192. The laws do not permit Microsoft to define the permissible bounds as whatever data  
10 practices are most commercially beneficial to Microsoft to avoid obtaining parental consent and  
11 compensating students.

12 **1. Parents have no knowledge of the full extent of Microsoft's true data**  
13 **practices and would find them highly offensive.**

14 193. Microsoft refused to disclose to Plaintiffs' parents the personal data it collected from  
15 or about Plaintiffs and how that personal data was used and shared.

16 194. Under COPPA, Microsoft is required to grant parents of children under 13 access to  
17 this information. However, Microsoft has a policy and practice of refusing to accommodate those  
18 requests.

19 195. For example, Plaintiffs H.W.1 and H.W.2 are under 13. When Ms. Williams requested  
20 access to H.W.1's and H.W.2's personal information collected by Microsoft, Microsoft failed to  
21 comply with her requests in violation of COPPA.

22 196. Consequently, students and parents do not and cannot know the full extent of the  
23 personal information Microsoft generates and collects from them, whether that personal data is  
24 accurate, how that personal data is stored, how long that personal data is retained, who has accessed  
25 that personal data, or how that personal data or personal data-derivative information or products are  
26 used by Microsoft or third parties.

27 197. More specifically, parents have no access to the extensive telemetric data and

1 metadata Microsoft collects or to the ways in which Microsoft’s algorithms have shaped and  
2 generated further data about their children. They have no access to Microsoft’s derived insights about  
3 their children or backend logs that influence how their children are understood and treated. And they  
4 have no recourse if the generated data, insights, or logs contain errors.

5 198. Although Plaintiffs cannot know the full extent of the personal information taken  
6 from them by Microsoft, they base their allegations on Plaintiffs’ use of the Products, the design and  
7 mechanics of the Products, Microsoft’s business model, and expert analysis of certain Microsoft  
8 Products when in use.

9 **2. Microsoft’s Products as designed take and use student data in clear excess of**  
10 **that necessary to provide educational services to children.**

11 199. Microsoft’s Products are not necessary for students to experience a rigorous  
12 education. Long before Microsoft and other technology giants engineered data-mining systems and  
13 marketed them to K-12 schools, students were receiving valuable educational services.

14 200. Indeed, a growing body of research shows that those traditional educational services  
15 were in fact more effective in achieving positive student outcomes than today’s data-driven, privacy-  
16 invasive services.

17 201. Research reveals that, since 2012, when digital products began to proliferate in  
18 classrooms across the U.S. and around the world, children and adolescents have suffered a variety  
19 of academic, physical, and psychosocial harms.<sup>34</sup>

20 202. The transition to computer-based education that began in 2012 is correlated with a  
21 significant decline in student academic performance, both in the U.S. and abroad.

22 203. Dozens of countries, including the U.S., participate in the Program for  
23 International Student Assessment (“PISA”). Created by the Organization for Economic Co-operation  
24 and Development, PISA tests the skills and knowledge of 15-year-old students in mathematics,

25  
26 <sup>34</sup>Sharon Tsang, *Excessive use of electronic devices among children and adolescents is associated*  
27 *with musculoskeletal symptoms, visual symptoms, psychosocial health, and quality of life: a cross-*  
*sectional study*, PubMed (June 29, 2023), <https://pmc.ncbi.nlm.nih.gov/articles/PMC10338872/>

reading, and science, and asks subjective questions about students' wellbeing.

204. Since 2012, scores in math, reading, and science have steadily fallen. By 2021, scores had dropped to the lowest levels recorded since 2000.<sup>35</sup>

205. Trends in the U.S. show a similar drop in scores in math and reading. The Nation's Report Card shows that the steady gains in reading made by 13-year-old students in the U.S. since 1971 have been virtually erased since 2012.<sup>36</sup>

206. The most recent data from the Nation's Report Card shows that high-school seniors' reading scores have dropped from 288 in 2013 to 283 in 2024.<sup>37</sup>

207. Likewise, the Nation's Report Card shows that, after steadily improving since 1971, the math scores of 13-year-old students in the U.S. rapidly declined beginning in 2012 to their lowest levels since the early 1990s.<sup>38</sup>

208. Even as more K–12 schools adopted digital tools like Microsoft's Products, digital literacy rates among U.S. students declined.

209. The International Computer and Information Literacy Study ("ICILS") measures 13-year-olds' readiness for today's digital learning and working environments. American students' performance in the ICILS fell significantly from 2018 to 2023.<sup>39</sup> The U.S. average score for

---

<sup>35</sup>OECD (2023), *PISA 2022 Results (Volume I): The State of Learning and Equity in Education*, PISA, OECD Publishing, Paris, <https://doi.org/10.1787/53f23881-en>; OECD (2023), *PISA 2022 Results (Volume II): Learning During – and From – Disruption*, PISA, OECD Publishing, Paris, [https://www.oecd.org/en/publications/pisa-2022-results-volume-ii\\_a97db61c-en.html](https://www.oecd.org/en/publications/pisa-2022-results-volume-ii_a97db61c-en.html); Haidt, J., Rausch, Z. (2025), *An EdTech Tragedy*, After Babel, <https://www.afterbabel.com/p/edtech-tragedy>

<sup>36</sup> NCES (2023), *The Nation's Report Card: National Assessment of Educational Progress Long-Term Trend Assessment*, <https://www.nationsreportcard.gov/ltr/reading/scores-percentiles/?age=13>; Haidt, J., Rausch, Z. (2025), *An EdTech Tragedy*, After Babel, <https://www.afterbabel.com/p/edtech-tragedy>

<sup>37</sup>U.S. Department of Education, Institute of Education Sciences, National Center for Education Statistics, National Assessment of Educational Progress (NAEP), 2002, 2005, 2008, 2013, 2015, 2019, and 2024 Reading Assessments

<sup>38</sup> NCES (2023), *The Nation's Report Card: National Assessment of Educational Progress Long-Term Trend Assessment*, <https://nces.ed.gov/nationsreportcard/data/>; Haidt, J., Rausch, Z. (2025), *An EdTech Tragedy*, After Babel, <https://www.afterbabel.com/p/edtech-tragedy>.

<sup>39</sup>NCES, ICILS 2023 U.S. Results, <https://nces.ed.gov/surveys/icils/icils2023/international.asp> (last visited Aug. 1, 2026);

1 computer and information literacy in 2023 was 482, down 37 points from an average score of 519  
2 in 2018.<sup>40</sup> The U.S. average score for computational thinking in 2023 was 461, also down 37  
3 points from an average score of 498 in 2018.<sup>41</sup>

4 210. These declines in academic performance occurred even as per-pupil expenditures  
5 among K–12 students in the U.S. increased 56 percent since 2013, which includes expenditures on  
6 educational technology such as Microsoft’s Products.<sup>42</sup>

7 211. The evidence does not suggest that Microsoft’s Products have benefited children’s  
8 academic performance.

9 212. Microsoft may not take and use student data as it sees fit under the guise of  
10 educational purposes and benefits.

11 213. Further, in taking data from children under 13 that far exceeds that necessary to  
12 provide education services, Microsoft violates COPPA’s data-minimization requirements.

### 13 **3. Microsoft’s data practices are unfair and unjust.**

14 214. Microsoft has generated massive profits through its generation, collection, and  
15 analysis of children’s personal information—without their parents’ knowledge or consent, and  
16 without compensating them for actively and passively providing Microsoft that valuable information  
17 and labor.

18 215. This one-sided arrangement—whereby Microsoft earns vast revenues each year using  
19

---

20 NCES, ICLS 2018 U.S. Results, <https://nces.ed.gov/surveys/icils/icils2018/theme1.asp> (last visited  
21 Aug. 1, 2026);

22 Merod, A., *8th graders’ average scores decline on computer and information literacy exam*,  
K12Dive (Nov. 12, 2024), <https://www.k12dive.com/news/computer-literacy-us-scores-icils-nces/732613/>.

23 <sup>40</sup>*Id.*

24 <sup>41</sup>*Id.*

25 <sup>42</sup> Edunomics Lab (2024), *ROI Over Time 2013-2024*, <https://edunomicslab.org/roi-over-time/> (last  
26 visited Aug. 1, 2026); Analysis by Edunomics Lab using data from these sources: Scores: The  
27 Nation’s Report Card  
(NAEP) 2013–2024; Spending: U.S. Census Annual Survey of School System Finances through  
2023; Inflation: CPI, BLS.

1 the personal information and labor of children gathered through children's compelled use of  
2 Microsoft Products, and all that children receive in return are education services to which they are  
3 already legally entitled—is particularly unjust given the core philanthropic purpose and compulsory  
4 nature of a public education.

5 216. Through its surreptitious, exploitative data practices, Microsoft has unjustly enriched  
6 itself at the cost of children's privacy, security, and autonomy, when children would otherwise have  
7 the ability to choose how they would monetize their data and labor—or decide not to. School-aged  
8 children, including Plaintiffs, should not be made to bear these risks and harms for the commercial  
9 benefit of private, for-profit corporations like Microsoft.

10 **I. Microsoft ignores legal limits and purports to dictate societal standards around student**  
11 **privacy.**

12 217. Student information collection and use practices that exceed the bounds of the law  
13 require parental consent. And for students under 13, COPPA's heightened standards require that  
14 Microsoft and other companies provide parents with notice and obtain their consent before  
15 collecting, using, and disclosing their young children's personal information and provide them with  
16 access to the collected information.

17 218. Furthermore, Microsoft's data practices are directly in violation of the MHMDA. The  
18 MHMDA requires entities like Microsoft to obtain affirmative consent before collecting consumer  
19 health data, maintain a consumer health data privacy policy that clearly identifies what health  
20 information is being collected and for what purpose, and establish data security practices that protect  
21 the confidentiality, integrity, and accessibility of consumer health data.

22 219. By collecting and maintaining Plaintiffs' and Class Members' sensitive medical and  
23 health information, without first obtaining their affirmative consent and establishing data security  
24 practices to protect the confidentiality, integrity, and accessibility of their health data, Microsoft is  
25 in violation of the MHMDA.

26 ///

27 ///

220. Microsoft disregards all existing legal limitations and acts as though it alone defines the standard for what can be taken from children without consent and how the information can be used.

221. A proper definition of the bounds of student-information practices includes many details: the types of information collected, how much information is collected, how it is collected, by whom, and for what purpose; where it is stored, how it is stored, and how long it is retained; who has access to it and how it is used by those with access; and with whom it is shared, how it is shared, how the receiving party stores it, and how the receiving party uses it.

222. Microsoft's system and policies intentionally and impermissibly obscure these details to the detriment of the children required to use its Products.

223. Microsoft has unlawfully expanded student surveillance, reduced student autonomy, altered and changed the course of students' educational experiences, and made participation in public education conditional on data exploitation.

224. Microsoft treats students and their parents as though their rights are wholly subordinate to its own business interests. It claims for itself the right to set the standard of what can be done in the name of “educational interests,” and it sets the standard at whatever is commercially beneficial to itself and its business interests.

225. Existing laws do not permit Microsoft to seize control of public-education data standards and trample on the rights of Washington students and their parents.

## CLASS ACTION ALLEGATIONS

226. Class Definition. Under Civil Rule 23(a) and (b)(3), Plaintiffs bring this case as a class action against Defendant on behalf of a statewide class of students (“the Class”) preliminarily defined as follows:

*All citizens of the state of Washington who attend or attended a K-12 school who used one or more Microsoft products.*

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

1           228. Members of the Class are collectively referred to herein as “Class members.”

2           229. Excluded from the Class are: (1) the Court (including any Judge or Magistrate  
3 presiding over this action and any members of their chambers and families); (2) Microsoft, its  
4 subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them  
5 have a controlling interest and its officers, directors, employees, affiliates, or legal representatives;  
6 (3) persons who properly and timely request exclusion from the Class; (4) persons whose claims in  
7 this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs’ counsel,  
8 Class’s counsel, and Microsoft’s counsel; and (6) the legal representatives, successors, and assigns  
9 of any such excluded person.

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

14           231. **Numerosity:** Members of the Class are so numerous that joinder of all members is  
15 impracticable. The exact size of the Class and the identities of the members of the Class are readily  
16 ascertainable in or through Microsoft’s records.

17           232. **Typicality:** Plaintiffs’ claims are typical of the claims of other members of the Class,  
18 as all members of the Class were uniformly affected by Microsoft’s wrongful conduct in violation  
19 of federal and state law as described herein.

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

26           234. **Commonality:** Common questions of law and fact exist as to all members of the  
27 Class and predominate over any questions affecting solely individual members of the Class.

Common questions for the Class include, but are not limited to, the following:

- a. What categories of personal information Microsoft collected, generated, and derived from students through their use of the Products;
- b. Whether Microsoft's collection, generation, and use of student data was uniform across student accounts by virtue of the common design, default settings, and operation of the Products;
- c. Whether Microsoft aggregated student data into individual student profiles and used those profiles and data for its own commercial purposes, including analytics, product development and improvement, algorithm and artificial-intelligence development, and marketing;
- d. Whether Microsoft obtained effective consent to collect, generate, and use Class members' personal information, including whether any consent given by school districts could or did extend to Microsoft's collection and use of student data for its own commercial purposes;
- e. Whether Microsoft's representations regarding its student-data practices — including that student data is collected and used only for educational purposes and remains under schools' control — were false, misleading, or rendered misleading by omission;
- f. Whether Microsoft's student-data practices constitute unfair or deceptive acts or practices in trade or commerce, affecting the public interest, in violation of the Washington Consumer Protection Act, RCW § 19.86.020;
- g. Whether Microsoft collected "consumer health data," as defined by RCW § 19.373.010(8), from Class members — including health information contained in education records, students' self-reported emotional states, and inferences regarding students' mental health and well-being — without the consent, privacy policy, and data-security practices required by chapter 19.373 RCW, and whether such violations constitute *per se* violations of the Consumer Protection Act pursuant to RCW § 19.373.090;
- h. Whether Microsoft's systematic collection, tracking, and profiling of students constitutes an intentional intrusion into Class members' private affairs;
- i. Whether Microsoft's conduct would be highly offensive to a reasonable person;
- j. Whether Class members' personal information and the data-generating activity Microsoft extracted from them conferred a benefit on Microsoft, whether Microsoft appreciated and retained that benefit, and whether its retention without payment is inequitable;
- k. Whether Microsoft concealed its student-data practices from students, parents, and schools;
- l. Whether Class members' personal information has economic value, and the appropriate class-wide methods for measuring that value, Class members' damages, and the restitution or disgorgement of Microsoft's unjustly obtained gains; and
- m. Whether Plaintiffs and Class members are entitled to injunctive and declaratory relief

1 requiring Microsoft to cease the unlawful practices alleged herein and to delete the  
2 student data and profiles it unlawfully collected and created.

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

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

#### 14 **V. TOLLING OF THE STATUTE OF LIMITATIONS**

15 237. Any applicable statute(s) of limitations have been tolled by Microsoft's and its  
16 affiliates' knowing and active concealment and denial of the facts alleged herein. Plaintiffs and  
17 members of the Class had no way of knowing and could not have reasonably discovered about  
18 Microsoft's data-harvesting scheme because Microsoft purposely concealed it. Plaintiffs' claims  
19 were thus tolled under the discovery rule.

20 238. The causes of action alleged herein did not accrue until Plaintiffs and members of the  
21 Class discovered or could have discovered Microsoft's data-harvesting scheme.

22 239. To this day, Microsoft fails to disclose the full extent of, and risks associated with, its  
23 data-harvesting scheme.

24 240. Within any applicable statutes of limitation, Plaintiffs and members of the Class could  
25 not have discovered, through the exercise of reasonable diligence, that Microsoft was concealing the  
26 conduct complained of herein.  
27

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

8           242. For most students and parents, the existence of the data-harvesting scheme is still  
9 unknown. For these reasons, all applicable statutes of limitation have been tolled by operation of the  
10 discovery rule with respect to the claims in this litigation.

11           243. In addition, and independently of the discovery rule and Microsoft's fraudulent  
12 concealment, all applicable statutes of limitations are tolled by RCW § 4.16.190. Under that statute,  
13 when a person entitled to bring an action is under the age of eighteen years at the time the cause of  
14 action accrues, the period of minority "shall not be a part of the time limited for the commencement  
15 of action."

16           244. Plaintiffs and Class members were minors under the age of eighteen at the time their  
17 causes of action accrued, because Microsoft collected, generated, and used their personal  
18 information while they were students enrolled in Washington K-12 schools. Each Plaintiff remains  
19 a minor today.

20           245. Accordingly, the limitations period applicable to each of Plaintiffs' and Class  
21 members' claims did not begin to run, and, for Plaintiffs and all Class members who remain under  
22 the age of eighteen, still has not begun to run, until the individual reached the age of eighteen. For  
23 Class members who have since reached the age of majority, the limitations period has still been  
24 tolled due to the discovery rule and Microsoft's fraudulent concealment, described above.

25 ///

26 ///

27 ///

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

**VI. CAUSES OF ACTION**

**Count I: Violation of the Washington Consumer Protection Act (CPA)**  
**Wash. Rev. Code Ann. §§ 19.86.020, *et seq.***  
***(On behalf of Plaintiffs and the Class Pursuant to Washington Law)***

246. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though fully set forth herein.

247. Microsoft is a “person,” as defined by Wash. Rev. Code Ann. § 19.86.010(1).

248. Microsoft advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

249. The CPA prohibits unfair or deceptive acts or practices in the conduct of trade or commerce. Wash. Rev. Code Ann. § 19.86.020. By engaging in the practices aforementioned, Microsoft has violated the CPA.

250. Microsoft’s unfair acts and practices include its violation of property, economic, and privacy interests protected by federal and state laws.

251. 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 Microsoft’s practices on school-aged children and their parents far outweighs the reasons, justifications, and motives of Microsoft.

252. The foregoing allegations also establish that Microsoft’s acts and practices were deceptive, as Microsoft’s omissions in actively concealing its true data practices were material, and they were likely to and did mislead some members of the public and/or caused harm to the public interest. They also misled parents, whether directly or indirectly through school personnel.

253. Microsoft’s unfair and deceptive acts and practices described herein emanated and were directed from Washington, where Microsoft is headquartered and where its leadership and employees created and approved those unfair and deceptive acts and practices.

1           254. Microsoft's unfair and deceptive acts and practices described herein directly or  
2 indirectly affected (and continue to affect) the people of Washington, as thousands of Washington  
3 residents are Class members and were, like Plaintiffs, harmed by those acts and practices.

4           255. Microsoft's conduct is unfair and has the capacity to deceive a substantial portion of  
5 the public. Microsoft markets its products to K-12 schools, represents that the data it collects is used  
6 solely for educational purposes when it is not, and intentionally fails to reveal the materially  
7 important facts that it collects, generates and retains far more student data than educational purposes  
8 require and uses this data for its own commercial purposes, including for targeted advertising and  
9 content, and developing and improving its Products.

10           256. Microsoft's conduct is unfair and injurious to the public interest because it violates  
11 Wash. Rev. Code Ann. § 19.86.020 and violates a statute that contains a specific legislative  
12 declaration of public interest impact, including, but not limited to Wash. Rev. Code Ann. §§ 19.375,  
13 *et seq.* Microsoft's telemetry systems capture detailed input behavior—including keystroke  
14 patterns—which are automatically measured and linked to individual user accounts. These patterns  
15 reflect biologically unique behavioral traits and are used, directly or indirectly, to identify, profile,  
16 and/or authenticate users across Microsoft services. As such, this collection constitutes enrollment  
17 of biometric identifiers without consent, in violation of Wash. Rev. Code Ann. § 19.375.

18           257. Microsoft's conduct is also unfair, deceptive, and injurious to the public interest  
19 because it violates common-law protections against invasion of privacy and COPPA by failing to  
20 provide parents with notice of its data practices, failing to obtain parental consent to its data practices,  
21 and actively denying parents' requests for the data Microsoft collects from and about their children.

22           258. Alternatively, Defendant's conduct is injurious to the public interest because it has  
23 injured Plaintiffs and Class members and has the capacity to injure other persons.

24           259. Defendant's violation of the MHMDA, a statute designed to recognize and protect  
25 the fundamental privacy rights of Washingtonians, also constitutes a *per se* violation of the CPA.

26           260. Plaintiffs and Class members suffered injury to their property in at least the following  
27 respects: (a) the taking, without consent or compensation, of personal information having a market

1 value that Microsoft itself establishes and pays through its Rewards program; (b) the loss of the  
2 opportunity to withhold, control, or monetize that information; and (c) the diminution in value of  
3 their personal information caused by Microsoft's collection, aggregation, use, and disclosure of it.  
4 These injuries are concrete and quantifiable, including by reference to the per-user value Microsoft  
5 pays Rewards participants for equivalent data.

6 261. Microsoft's actions caused damage to and loss of Plaintiffs' and Class members'  
7 property right to control the dissemination and use of their personal information and  
8 communications.

9 262. If not for Microsoft's unfair and deceptive acts and practices, Plaintiffs and Class  
10 members would not have had their personal information taken without consent via Microsoft's  
11 Products used in schools, and Plaintiffs and Class members would not have suffered the above-  
12 described injuries.

13 263. Microsoft's unfair and deceptive acts and practices proximately caused Plaintiffs' and  
14 Class members' injuries through a direct and foreseeable causal chain: Microsoft made the  
15 misrepresentations and material omissions described above to Washington school districts,  
16 educators, and the public; in reliance on those representations, Plaintiffs' school district and districts  
17 across Washington licensed and deployed the Products and required students to use them; Plaintiffs  
18 and Class members, compelled to use the Products as part of their education, thereby had their  
19 personal information taken, profiled, and commercially exploited without consent and without  
20 compensation. But for Microsoft's misrepresentations and concealment, districts would not have  
21 deployed the Products on these terms, parents would have had the opportunity to withhold consent,  
22 and Microsoft could not have obtained Plaintiffs' and Class members' data.

23 264. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by  
24 law, including actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

25 ///

26 ///

27 ///

1           265. Microsoft reaped unjust profits and revenues in violation of the CPA. This includes  
2 Microsoft's profits and revenues from its improvements to and development of Microsoft's other  
3 products. Plaintiffs and the Class seek restitution and disgorgement of these unjust profits and  
4 revenues.

5                   **COUNT II: Invasion of Privacy—Intrusion Upon Seclusion**  
6                   ***(On behalf of Plaintiffs and the Class Pursuant to Washington Law)***

7           266. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though  
8 fully set forth herein.

9           267. Under Washington law, Plaintiffs asserting claims for intrusion upon seclusion must  
10 plead (1) intentional intrusion into the plaintiffs' private affairs or concerns; (2) in a manner highly  
11 offensive to a reasonable person.

12           268. Microsoft intentionally intruded into Plaintiffs' and Class members' private affairs in  
13 a highly offensive manner through its systematic and pervasive collection, accessing, downloading,  
14 transferring, storing and use of Plaintiffs' and Class members' personal information.

15           269. The intrusion alleged is not the school's supervision of schoolwork—which students  
16 and parents expect—but Microsoft's covert extraction, for its own commercial purposes, of  
17 behavioral, telemetric, and inferred data that no student or parent knew existed. No reasonable  
18 student expects that the speed of her typing, the pressure of her clicks, the pattern of her scrolling,  
19 and inferences about her emotional state, among many other personal and sensitive categories of  
20 data, are being continuously harvested by a private corporation and assembled into a persistent  
21 commercial profile.

22           270. Plaintiffs and Class members maintained a reasonable expectation of privacy in their  
23 personal information absent consent to tracking and collection practices. Plaintiffs and Class  
24 members never consented or even had the opportunity to consent to Microsoft's data practices related  
25 to Microsoft products used by schoolchildren at school.

26           ///

27           ///

1           271. The reasonableness of this expectation of privacy is reflected in COPPA, which  
2 prevents the collection, use, and sharing of personal information of children under 13 by private  
3 companies without parental consent.

4           272. Plaintiffs' and Class members' reasonable expectation of privacy in their personal  
5 information is further supported by longstanding custom and practice; security measures intended to  
6 prevent unauthorized access to personal information, especially concerning young children; state  
7 and federal laws protecting children's and adults' personal information in their health and other  
8 records; among other indicia.

9           273. Plaintiffs and Class members could not reasonably expect that, by simply  
10 participating in their education and completing required school activities, Microsoft would collect,  
11 store, manipulate, and monetize such voluminous and far-reaching categories of personal  
12 information; prevent Plaintiffs and Class members from reviewing, correcting, or controlling that  
13 information; and use that information in ways that were harmful to Plaintiffs and Class members.

14           274. Individuals also maintain a reasonable expectation of privacy when they are using  
15 products in a compulsory environment such as public schools. Microsoft's collection of Plaintiffs'  
16 and Class members' information while logged into Microsoft products at school was unreasonable.

17           275. Plaintiffs' and Class members' expectation of privacy did not diminish because  
18 Microsoft's surveillance occurred through school-issued devices and school-required accounts.  
19 Students used the Products for quintessentially private activities: composing personal  
20 communications; conducting internet searches reflecting their curiosities, anxieties, health concerns,  
21 and beliefs; responding to social-emotional check-ins about their feelings; and creating schoolwork  
22 revealing their thoughts and opinions. Until 2025, Plaintiffs used their school-issued devices at  
23 home—in their bedrooms and family spaces—for homework and the internet activity that  
24 accompanied it. A child does not surrender her expectation of privacy in her thoughts, feelings,  
25 searches, communications, and physical behaviors as the price of attending public school; if  
26 anything, the compulsory setting heightens the expectation that information generated there will be  
27 used only for education.

1           276. Microsoft's collection and use of children's personal information without the  
2 knowledge or consent of those children or their parents is highly offensive to a reasonable person.

3           277. COPPA demonstrates that students under the age of 13 have a reasonable expectation  
4 of privacy in their personal information while using online services in schools, and Microsoft's  
5 collection and use of Plaintiffs' personal information without providing notice to Plaintiffs' parents  
6 and without obtaining verifiable parental consent in violation of COPPA is highly offensive to a  
7 reasonable person.

8           278. Microsoft's intrusions upon Plaintiffs' and Class members' private affairs and  
9 concerns are highly offensive to a reasonable person, especially considering (a) the highly sensitive  
10 and personal nature of Plaintiffs' and Class members' personal information and data, including  
11 behavioral, social-emotional, and telemetric data; (b) the extensive scope of data obtained by  
12 Microsoft, including years of historical data and far more data than is reasonably necessary for  
13 legitimate educational purposes; (c) Microsoft's intent to profit from Plaintiffs' and Class members'  
14 data by using it to develop and market its products and services; (d) Microsoft's use of subterfuge to  
15 intrude into Plaintiffs' and Class members' electronic devices for the purpose of collecting their data;  
16 (e) the surreptitious and unseen nature of Microsoft's data collection with respect to consumers, (f)  
17 Microsoft's failure to provide parents with notice of its data practices, and (g) Microsoft's failure to  
18 obtain effective consent.

19           279. Microsoft's conduct would be highly offensive to a reasonable person, particularly  
20 given that Microsoft designs products to be used by children, including young children. The manner  
21 of the invasion—collection through students' use of education tools in a compulsory setting—is also  
22 highly offensive.

23           280. Microsoft's invasions of privacy caused Plaintiffs and Class members the following  
24 damages:

- 25           a. Nominal damages;
- 26           b. The diminution in value of Plaintiffs' and Class members' private information;
- 27           c. The loss of privacy due to Microsoft rendering no longer private the confidential and  
personal information that Plaintiffs and Class members intended to remain private; and

1 d. The fair value of Plaintiffs' and Class members' personal information and data. Microsoft  
2 took something of value from Plaintiffs and Class members—their personal information  
3 and data—and derived benefits therefrom without Plaintiffs' and Class members'  
4 knowledge or consent and without Microsoft sharing the fair benefit of such value with  
5 them.

6 281. Microsoft's intrusions also caused Plaintiffs and Class members the harms that the  
7 tort of intrusion exists to remedy: the loss of solitude and seclusion; the anxiety, discomfort, and  
8 distress that flow from pervasive covert surveillance during childhood; and the affront to personal  
9 dignity and autonomy inherent in being watched, measured, profiled, and predicted without  
10 knowledge or consent throughout one's formative years.

11 282. As a result of Microsoft's invasions of privacy, Plaintiffs and Class members seek  
12 actual damages, compensatory damages, restitution, disgorgement, general damages, nominal  
13 damages, unjust enrichment, and any other relief the Court deems just.

14 **COUNT III: Unjust Enrichment**  
15 ***(On Behalf of Plaintiffs and the Class Pursuant to Washington Law)***

16 283. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though  
17 fully set forth herein.

18 284. Plaintiffs lack an adequate remedy at law.

19 285. In addition, or as an alternative to legal remedies sought herein, Plaintiffs seek  
20 equitable relief to the extent that legal remedies are inadequate.

21 286. Under Washington law, Plaintiffs asserting claims for unjust enrichment must plead:  
22 (1) the plaintiff conferred a benefit on the defendant, (2) the defendant had appreciation or  
23 knowledge of the benefit, and (3) under the circumstances, the defendant's acceptance or retention  
24 of the benefit makes it inequitable for defendant to retain the benefit without payment of its value.  
25 Washington courts have also at times included an element that the benefit conferred be at the expense  
26 of the plaintiff.

27 287. Plaintiffs conferred a benefit upon Microsoft, namely, provision of their personal  
information and labor to Microsoft through their compelled use of Microsoft's Products at school.

28 288. Microsoft appreciated the fact that it obtained these benefits from Plaintiffs, namely,

1 it understands that student data and usage and other metrics are a large part of the raw material that  
2 fuels its business, without which Microsoft would have fewer and less-developed products and  
3 significantly lower profits.

4 289. It would be inequitable for Microsoft to retain those benefits without payment to  
5 Plaintiffs of the value the benefits have conferred to Microsoft because Plaintiffs and Class members  
6 are schoolchildren who conferred the benefits through their required participation in educational  
7 activities at school and related to school, and Microsoft failed to obtain the necessary parental  
8 consent in violation of federal and state law.

9 290. The benefit conferred by Plaintiffs and Class members to Microsoft was conferred at  
10 Plaintiffs' and Class members' expense because their personal information and labor have economic  
11 value as recognized by Washington courts and as demonstrated by the market value Microsoft itself  
12 establishes and pays through its Rewards program for equivalent data and by Microsoft's commercial  
13 use of the data and labor for the development, improvement, and marketing of its products. More  
14 specifically, Microsoft acquired and compromised troves of personal information that rightfully  
15 belong to Plaintiffs and Class members and used the fruits of Plaintiffs' and Class members' labor  
16 without effective consent through intentionally unfair and deceptive practices conducted in  
17 connection with students' compulsory use of Microsoft's products.

18 291. Microsoft obtained access to this information and labor only by marketing,  
19 distributing, and selling its products for use by children in the compulsory environment of K-12  
20 education.

21 292. Microsoft has built, developed, improved, marketed, and delivered an ever-growing  
22 suite of products using the personal information and labor of Plaintiffs and Class members. It has  
23 further derived profits and other tangible and intangible benefits from its improper collection and  
24 use of Plaintiffs' and Class members' data and labor.

25 ///

26 ///

27 ///

1           293. Collecting children’s personal information and using their labor without effective  
2 consent has allowed Microsoft to grow its business, acquire numerous other tangible and intangible  
3 assets, develop other applications, and as of the date of this filing, stand at more than a trillion-dollar  
4 valuation.

5           294. Microsoft has also directly and substantially profited from its use, storage, and  
6 aggregation of Plaintiffs’ and Class members’ data and labor. Indeed, Plaintiffs’ and Class members’  
7 data and labor helps power Microsoft’s ever-growing ecosystem of products and services.

8           295. In exchange for these benefits to Microsoft, Plaintiffs and Class members received  
9 nothing but educational services to which they were already legally entitled and required to receive.

10          296. To benefit its bottom line, Microsoft deprived Plaintiffs and Class members of their  
11 property, security, privacy, and autonomy.

12          297. Microsoft harmed Plaintiffs and Class members by, among other harms, subjecting  
13 them to commercial manipulation and continuous surveillance; invading their privacy; subjecting  
14 them to opaque, unreviewable data practices; forcing them to choose between their right to an  
15 education and other fundamental rights; and failing to compensate them for their property and labor.

16          298. Neither Plaintiffs and Class members nor their parents consented to Microsoft’s  
17 taking of their personal information and labor and using it for Microsoft’s commercial gain.

18          299. Plaintiffs and Class members are not parties to any contract with Microsoft.  
19 Microsoft’s agreements are with school districts. Plaintiffs never saw, negotiated, or assented to those  
20 agreements or to any Microsoft terms of service, and their accounts were created for them by their  
21 schools without any terms being presented to them or their parents. No contract governs the  
22 relationship between Microsoft and Plaintiffs with respect to the conduct alleged, and no contractual  
23 remedy exists for it.

24          300. To the extent Microsoft contends that any Microsoft terms bind Plaintiffs or Class  
25 members, Plaintiffs and Class members are minors who never received or assented to such terms,  
26 and they hereby disaffirm, to the fullest extent permitted by law, any agreement Microsoft claims  
27 they entered.

1           301. There is no justification for Microsoft’s enrichment. It would be inequitable,  
2 unconscionable, and unjust for Microsoft to be permitted to retain these benefits when they were  
3 procured because of and by means of Microsoft’s wrongful conduct and at the expense of children’s  
4 property and wellbeing.

5           302. Plaintiffs and Class members seek an order compelling Microsoft to disgorge the  
6 profits and other benefits it has unjustly obtained.

7           303. Plaintiffs and Class members lack an adequate remedy at law for this claim.  
8 Microsoft’s conduct is ongoing and the benefit Microsoft receives—the incorporation of Plaintiffs’  
9 and Class members’ data and its derivatives into Microsoft’s profiles, analytics, algorithms, models,  
10 and products—is continuing and compounding in ways that damages measured at law cannot  
11 capture. The value Microsoft has extracted resides in Microsoft’s own systems and business, in  
12 amounts known to Microsoft and not to Plaintiffs, and is properly measured by Microsoft’s gains  
13 (through restitution and disgorgement) rather than by Plaintiffs’ losses.

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

17           **COUNT IV: Violation of Washington’s My Health My Data Act (“MHMDA”)**  
18                               **Wash. Rev. Code Ann. §§ 19.373, et seq.**  
19                               **(On Behalf of Plaintiffs and the Class Pursuant to Washington Law)**

20           305. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as though  
21 fully set forth herein.

22           306. Plaintiffs and Class members are “consumers” within the meaning of RCW §  
23 19.373.010(7) as natural persons who are Washington residents or natural persons whose consumer  
24 health data is collected in Washington.

25           307. Microsoft collected and used “consumer health data” within the meaning of RCW §  
26 19.373.010(8) by obtaining personal information that is linked or reasonably linkable to a consumer  
27 and identifies the consumer’s past, present or future physical or mental health status from Plaintiffs  
and Class Members.

1           308. Microsoft is a “regulated entity” within the meaning of RCW § 19.373.010(23) as an  
2 entity that conducts business in Washington and alone determines the purpose and means of  
3 collecting, processing, sharing, or selling consumer health data.

4           309. Since March 31, 2024, the effective date of the MHMDA’s obligations for regulated  
5 entities, Microsoft has collected Plaintiffs’ and Class members’ consumer health data without  
6 obtaining their (or their parents’) affirmative, voluntary consent as required by RCW § 19.373.030;  
7 it has failed to maintain a consumer health data privacy policy meeting the requirements of RCW §  
8 19.373.020; and it has failed to restrict internal access to and establish required security practices for  
9 such data as required by RCW § 19.373.050.

10           310. On information and belief, Microsoft has also shared Plaintiffs’ and Class members’  
11 consumer health data—including with processors, vendors, and affiliated services—without the  
12 consent of Plaintiffs, Class members, or their parents, and has engaged in the processing of such data  
13 for its own commercial purposes that exceeds any legitimate educational purposes and any consent  
14 given by a school or school district, which consent is in any case ineffective and insufficient under  
15 the MHMDA.

16           311. Prior to obtaining and using Plaintiffs’ and Class members’ personal data, Microsoft  
17 never obtained consent, nor did Defendant clearly and conspicuously disclose the categories of  
18 Plaintiffs’ and Class members’ health data collected, the purpose of the collection of their health  
19 data, or how they can withdraw consent from future collection.

20           312. Pursuant to RCW § 19.373.090, a violation of the MHMDA “is an unfair or deceptive  
21 act in trade or commerce and an unfair method of competition for the purpose of applying the  
22 consumer protection act, chapter 19.86 RCW,” and the practices covered are declared matters  
23 “vitally affecting the public interest.” Plaintiffs assert this Count through chapter 19.86 RCW and  
24 incorporate the injury and causation allegations of Count I.

25           313. Plaintiffs seek all monetary and non-monetary relief allowed by law.

26 ///

27 ///

1 **VII. RELIEF REQUESTED**

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

- 4 a. An award of damages, including actual, compensatory, general, special, incidental,  
5 consequential, and treble damages, as well as restitution and disgorgement, in an amount  
6 to be determined at trial;
- 7 b. Injunctive, declaratory, and other equitable relief as appropriate;
- 8 c. Pre- and post-judgment interest to the extent provided by law;
- 9 d. Attorneys' fees to the extent provided by law;
- 10 e. Costs to the extent provided by law; and
- 11 f. Such other relief the Court deems just and proper.

12  
13 Respectfully submitted,

14 Dated: August 14, 2026

15 By: /s/ M. Anderson Berry  
M. Anderson Berry (WA # 63160)

16 By: /s/ Brook Garberding  
17 Brook Garberding (WA # 37140)  
18 Gregory Haroutunian\*  
Brandon P. Jack\*  
**EMERY | REDDY, PC**  
600 Stewart Street, Suite 1100  
Seattle, WA 98101  
206.442.9106 (Tel)  
206.441.9711 (Fax)  
anderson@emeryreddy.com  
brook@emeryreddy.com  
gregory@emeryreddy.com  
brandon@emeryreddy.com

24 Julie U. Liddell\*  
25 W. Andrew Liddell\*  
Elizabeth Huddleston\*  
**EDTECH LAW CENTER PLLC**  
904 Rio Grande Street, Suite 100  
Austin, TX 78701  
737.351.5855 (Tel)

julie.liddell@edtech.law  
andrew.liddell@edtech.law  
beth.huddleston@edtech.law

Andrew R. Tate\*  
**PEIFFER WOLF CARR  
KANE CONWAY & WISE LLP**  
235 Peachtree St. NE, Suite 400  
Atlanta, GA 30303  
314.669.3600 (Tel)  
atate@peifferwolf.com

Karen Dahlberg O'Connell\*  
**ALMEIDA LAW GROUP LLC**  
157 Columbus Avenue, 4th Floor  
New York, NY 10023  
347.395.5666 (Tel)  
karen@almeidalawgroup.com

Lori G. Feldman (WA # 29096)  
**HECHT PARTNERS LLP**  
125 Park Avenue, 25<sup>th</sup> Floor  
New York, NY 10017  
212.851.6821 (Tel)  
lfeldman@hechtpartners.com  
e-servicecapg@hechtpartners.com

\* *pro hac vice* forthcoming

*Counsel for Plaintiffs and the Proposed Class*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Microsoft Collects 'Massive' Amounts of Info From K-12 Students Without Parental Consent, Class Action Lawsuit Claims](#)

---