Rebecca A. Peterson (241858)
RPeterson@4-justice.com
1650 West 82nd Street, Suite 880
Bloomington, MN 55431
Tel.: (612) 778-9595
Fax: (888) 421-4173

Lori G. Feldman (*pro hac vice* forthcoming)
LFeldman@4-justice.com
Michael Liskow (SBN 243899)
MLiskow@4-Justice.com
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel.: (917) 983-9321
Fax: (888) 421-4173

David J. George (*pro hac vice* forthcoming)
DGeorge@4-justice.com
Brittany Sackrin (*pro hac vice* forthcoming)
BSackrin@4-Justice.com
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Tel.: (561) 232-6002
Fax: (888) 421-4173
GEORGE FELDMAN MCDONALD, PLLC

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

Daniel E. Gustafson (*pro hac vice* forthcoming)
dgustafson@gustafsongluek.com
Catherine Sung-Yun K. Smith (*pro hac vice forthcoming)*
csmith@gustafsongluek.com
Shashi K. Gowda (*pro hac vice* forthcoming)
sgowda@gustafsongluek.com
Canadian Pacific Plaza
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
Tel.: (612) 333-8844
Fax: (612) 339-6622
GUSTAFSON GLUEK, PLLC

Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOEL SCHWARZ, on behalf of his minor child B.S., EMILY DUNBAR, on behalf of her minor child H.D., and MICHAEL GRIDLEY and ELIZABETH GRIDLEY, on behalf of their minor children A.G. and Z.G., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Civ. No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

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

- Thomas Jefferson to James Madison, 1787

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

- Jose Ferreira, EdTech CEO, May 2014

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

- Michael Moe, EdTech investor, May 2014

INTRODUCTION

1. Plaintiffs and the Class members bring this action against Defendant Google LLC ("Google") for acts in violation of various state and federal laws protecting children's privacy rights.

2. Google has built a multitrillion-dollar empire by monetizing vast troves of personal information from individuals—including millions of school-aged children—without effective consent.

3. Google's core business is generating and extracting as much information as possible about its users and exploiting that information for profit. The products it markets for use by children in K-12 education are no exception.

4. Google markets products to primary, secondary, and post-secondary schools around the world. Its products include the Chromebook, Chrome OS, the Chrome browser, and a suite of cloud-based web applications.

5. Through its products, Google surreptitiously surveils students and continually extracts their personal information. Google and its customers convert that information into intimately detailed profiles on school-aged children, which they use to market products and services to them, to manipulate how they think and act, to shape their information environment, and to make significant

decisions affecting their lives and their futures—all without students or their parents ever knowing or having an opportunity to avoid or limit the unauthorized collection and distribution of their children's personal and private information.

6. Google's massive data-harvesting apparatus exposes children to serious and irreversible risks to their privacy, property, and autonomy, and harms them in ways that are both concealed and profound.

7. Neither students nor their parents[1] have agreed to this arrangement. To be effective, an agreement must be supported by informed, voluntary consent by a person with authority to do so in exchange for sufficient consideration. None of those elements are met here.

8. Any purported agreement is not informed: Google does not disclose to students, parents, or schools what information it collects and what it does with that information.

9. Any purported agreement is not voluntary: because parents are required to send their children to school, they are coerced into submitting to Google's practices.

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

11. Any purported consent was not provided by a person with authority to do so. Because most users of Google's K-12 products are minors, Google is required to obtain parental consent before taking and using children's data. However, Google does not seek parental consent in taking children's personal information through its "Core Services" for Workspace for Education. Instead, Google relies on the consent of school personnel alone. But school personnel do not have authority to provide consent in lieu of parents. Thus, even if school personnel purport to have given consent on behalf of students, any such consent is ineffective.

12. Schools have always collected certain personal information about students, and they

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

must be able to continue to do so—within the bounds of the law.[2] Until recently, that collection was transparent and limited: parents generally knew what information was collected, by whom, and for what purpose. But times—and technology—have changed.

13. Schools no longer do the collecting; corporate third parties do. The information collected is not only traditional education records, but thousands of data points that span a child's life. The information taken is not used exclusively for educational purposes; it is used by private entities for commercial purposes. This extractive corporate business model does not prioritize positive student outcomes; it prizes "measurability," "scalability," and other corporate-profit imperatives that are often unaligned with, and are even adversarial to, healthy child development. Companies may not deny parents control over their children's lives by marketing to schools and concealing their practices behind opaque technology and empty promises of improving education.

14. Google itself has warned about "[t]he civil liberties and human rights concerns associated with" access to such "sensitive" information.[3] Google may not require that children forgo their rights so that they may receive the education to which they are legally entitled. And parents, by sending their children to school as is their right and duty, do not relinquish their authority to decide what information may be collected about their children and how it may be used. Google must be held to account for operating as though the fundamental rights of children and their parents do not exist.

[2] In this lawsuit, Plaintiffs do not seek to prevent schools from collecting and using legally permissible information about their students in a legally permissible manner, such as contemplated under the Family Educational Privacy and Rights Act ("FERPA").

[3] ACLU, *ECTR Coalition Letter* (June 6, 2016), https://www.aclu.org/documents/ectr-coalition-letter (last accessed April 4, 2025).

TABLE OF CONTENTS

15. Plaintiffs Joel Schwarz, on behalf of and as parent and guardian of his minor child B.S.; Emily Dunbar, on behalf of and as parent and guardian of her minor child, H.D.; and Michael Gridley and Elizabeth Gridley, on behalf of and as parents and guardians of their minor children A.G. and Z.G.; as well as on behalf of all other similarly situated individuals ("Plaintiffs"), by and through their attorneys, bring this class action complaint for injunctive and monetary relief under Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3) against Google LLC ("Google") and make the following allegations based upon knowledge as to themselves and the acts of themselves and their minor children, and upon information and belief as to all other matters, as follows:

JURISDICTION AND VENUE

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

17. Venue is proper in this District under 28 United States Code section 1391 because Google is subject to personal jurisdiction here, and regularly conducts business in this District, and because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

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

19. Moreover, one of Google's Terms of Service mandate that all "disputes will be resolved exclusively in the federal or state courts of Santa Clara County, California," and that Google

consents to personal jurisdiction in those courts. Google is headquartered in Santa Clara County, California, which is located within the Northern District of California.

THE PARTIES

20. Plaintiff B.S. is a minor. At all times relevant to the allegations set forth herein, she was and is domiciled in the state of Maryland. B.S. attended school in a public school district in Maryland. As part of her public schooling, she was required to access and use the Google Workspace for Education suite of applications and the Chrome browser, which she accessed and used from her school-issued device, a Google Chromebook.

21. Plaintiff Joel Schwarz is the father and legal guardian of Plaintiff B.S. At all times relevant to the allegations set forth herein, he was and is domiciled in the state of Maryland.

22. Plaintiff H.D. is a minor. At all times relevant to the allegations set forth herein, she was and is domiciled in the state of Oregon. H.D. attended school in a public school district in Oregon. As part of her public schooling, she was required to access and use the Google Workspace for Education suite of applications and the Chrome browser, which she accessed and used from her school-issued device, a Google Chromebook.

23. Plaintiff Emily Dunbar is the mother and legal guardian of Plaintiff H.D. At all times relevant to the allegations set forth herein, she was domiciled in the state of Oregon.

24. Plaintiff A.G. is a minor. At all times relevant to the allegations set forth herein, she was and is domiciled in the state of California. A.G. attends school in a public school district in California. As part of her public schooling, she is required to access and use the Google Workspace for Education suite of applications and the Chrome browser, which she accesses and uses from her school-issued device, a Google Chromebook.

25. Plaintiff Z.G. is a minor. At all times relevant to the allegations set forth herein, she was and is domiciled in the state of California. Z.G. attended school in a public school district in California. As part of her public schooling, she was required to access and use the Google Workspace for Education suite of applications and the Chrome browser, which she accessed and used from her school-issued device, a Google Chromebook.

26. Plaintiff Michael Gridley is the father and legal guardian of Plaintiffs A.G. and Z.G. At all times relevant to the allegations set forth herein, he was domiciled in the state of California.

27. Plaintiff Elizabeth Gridley is the mother and legal guardian of Plaintiffs A.G. and Z.G. At all times relevant to the allegations set forth herein, she was domiciled in the state of California.

28. Defendant Google was originally incorporated as Google Inc. in California in September 1998 and reincorporated in Delaware in August 2003. In or around 2017, Google Inc. converted to a Delaware limited liability company, Defendant Google, LLC (together collectively with its predecessor-in-interest Google Inc., "Google"). On October 2, 2015, Google reorganized and became a wholly owned subsidiary of a new holding company, Alphabet Inc., a Delaware corporation with its principal place of business in Mountain View, CA.

FACTUAL ALLEGATIONS

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

A. Google pioneered the data-monetization business model of the modern internet.

29. In 2003, shortly after its founding, Google developed a new economic model by which it gathered vast quantities of data from and about users, which it used to build detailed behavioral profiles of users. It then used, and eventually marketed, those profiles for precision-targeted advertising. The following year, Google became a publicly traded company. Google is now worth more than 1.8 trillion dollars, making it one of the most valuable companies the world has ever known.

30. In the decades since Google pioneered this business model, many other consumer-facing technology companies followed suit and built their businesses around what Harvard Business School professor emerita Shoshana Zuboff has described as "surveillance capitalism."[4] At the heart of that model is an "extraction imperative" that prioritizes maximal collection and monetization of user data at the expense of consumers' rights to privacy.

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

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

a. generate and collect as much data as possible about a user through the user's interaction with the technology provider's platform;

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

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

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

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

33. Given the extractive and exploitative nature of the surveillance business model,[5] its viability depends on keeping the public in the dark. Companies thus employ numerous tactics to keep users engaged and uninformed, such as opaque terms of service, clickwrap and browsewrap "agreements," hidden data-generation and data-collection technologies, and manipulative design techniques.

34. The practices of surveillance capitalism have become commonplace—not just in technological domains like search browsers, e-commerce, and social media—but also in more traditional domains such as healthcare, employment, lending, and insurance. Courts have routinely found undisclosed corporate practices in these domains to be unlawful. If this business model is unfair when used against adults in ostensibly voluntary consumer contexts, it is unconscionable when used against school-aged children in the compulsory setting of kindergarten through twelfth grade ("K-12") education.

[5] "Surveillance business model" and "data-monetization business model" are used interchangeably herein.

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

35. The surveillance business model also underpins digital products used in K-12 schools across the U.S., including Google's Products.[6]

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

37. Education has been described by one Educational Technology ("EdTech") executive as "the world's most data-mineable industry by far."[7]

38. Google has positioned itself, through its ever-growing suite of cloud-based applications, as the *de facto* platform through which an ever-growing number of other application providers inject their products into compulsory education environments for use by school-aged children.[8]

II. Google secretly collects and monetizes the personal and private information of millions of school-aged children.

39. Google's K-12-marketed products do not merely serve as a kind of digital filing cabinet in which schools may store education records.

40. Rather, Google generates, collects, and otherwise obtains personal information from, about, and belonging to tens of millions of school-aged children in the U.S.

41. Data generation, extraction, collection, analysis, and disclosure form the foundation

[6] As used herein, "Products" refers to Google's Chromebook, Chrome OS, Chrome browser, and Workspace for Education.

[7] Stephanie Simon, *The Big Biz of Spying on Little Kids*, POLITICO (May 15, 2014), https://www.politico.com/story/2014/05/data-mining-your-children-106676 (last accessed April 4, 2025).

[8] *The Implications for EdTech of Google's Market Share in Education*, VISTAPOINT ADVISORS (Jul 29, 2021), https://vistapointadvisors.com/news/implications-edtech-googles-market-share-education (last accessed April 4, 2025).

of Google's business model. And, true to its surveillance-capitalist imperative, Google has realized historic profits through its development and expansion of its unprecedented data-harvesting scheme.

42. In fact, Google's learning management system is the most used K-12 learning management system in the U.S.[9]

A. Google's products—including those marketed and sold to K-12 schools—are designed and optimized to generate and collect student data.

1. Google markets and sells products to K-12 schools.

43. Google markets and sells many products for use by students in the K-12 education setting, including the Chromebook laptop computer, Chrome OS, Chrome browser, and a suite of digital products known as Google Workspace for Education ("Workspace for Education") (collectively, "Google's Products" or "Products").

44. A Chromebook is a laptop computer that runs Chrome OS, Google's cloud-based operating system. While other companies manufacture Chromebooks, only Google designs Chrome OS.

45. Chrome OS is designed primarily to run web applications ("apps") through the Chrome browser.

46. The Chrome browser is Google's general web browser. Its primary purpose is to provide users access to the open internet, allowing users to view and interact with websites and web apps, such as those in Workspace for Education.

47. Workspace for Education is Google's suite of cloud-based web apps marketed for use by K-12 students. They are designed to run within a web browser, which is the Chrome browser by default. In other words, the Chrome browser is the primary gateway to Workspace for Education apps.[10]

---

[9] *The EdTech Top 40: A Look at K-12 EdTech Engagement During the 2023-24 School Year*, INSTRUCTURE, https://www.instructure.com/resources/research-reports/edtech-top-40-look-k-12-edtech-engagement-during-2023-24-school-year?filled (last accessed April 4, 2025).

[10] Although Workspace for Education apps may be accessed through different operating systems and on different browsers, this complaint concerns only those running on Chrome OS and the Chrome browser—the default manner of accessing those apps.

48. Nearly 70 percent of K-12 schools in the U.S. use Workspace for Education.[11]

49. Google offers different editions of Workspace for Education. The most basic edition is branded Google Workspace for Education Fundamentals. Google offers that edition at no cost to K-12 schools that are "government-recognized, accredited schools" that have "an active website" and that have the application submitted by a member of the school. Google also offers other editions at a cost. Those include Google Workspace for Education Standard; the Teaching and Learning Upgrade; and Google Workspace for Education Plus.

50. On information and belief, the quality and quantity of data Google generates about and collects from students is the same across editions.

51. Every edition of Workspace for Education includes the following web apps among its "Core Services" apps:

a. **Gmail** is an email service for students and staff.

b. **Google Calendar** is a calendar for scheduling classes, meetings, and events.

c. **Google Drive** is a cloud storage for documents, files, and other data.

d. **Google Docs** is a document creation and editing tool.

e. **Google Sheets** is a spreadsheet tool for data analysis and calculations.

f. **Google Slides** is a presentation creation and editing tool.

g. **Google Forms** is a form creation tool for surveys, quizzes, and data collection.

h. **Google Tasks** is a task management tool.

i. **Google Classroom** is a classroom management tool for organizing assignments, discussions, and materials.

j. **Google Meet** is a video conferencing tool for online meetings and classes.

k. **Google Sites** is a website creation tool for building websites.

[11] *How Google Conquered the Classroom: The Googlification of Schools Worldwide for 2025*, RESEARCH.COM (Mar. 12, 2025), https://research.com/education/how-google-conquered-the-classroom#:~:text=Indeed%2C%20EdWeek%20Market%20Brief%20(2017,use%20Chromebooks%20frequently%20for%20instruction. (last accessed April 4, 2025).

l. **Google Gemini** is a generative artificial-intelligence tool (with additional data protection available in paid editions).

m. **Google Contacts** is a contact management tool.

n. **Google Chat** is a communication and collaboration tool for teams.

o. **Google Groups** is a service for online discussion groups.

p. **Google Keep** is a note-taking app.

q. **Google Read Along** is an AI-based language-learning application that helps students learn to read using a virtual speech-based tutor that provides "auto-generated insights" about users.

r. **Google Vault** is a cloud-based archiving and e-discovery service.

s. **Google eDiscovery** is a tool for searching, holding, and exporting data from Workspace apps for legal and compliance purposes.

t. **Chrome Sync** is a feature that allows users to synchronize bookmarks, history, passwords, and other settings across all devices where they are signed into Chrome.

u. **Cloud Identity Services** is a centralized identity-management platform for organizations (advanced security and control features available for a charge).

v. **Google Workspace LTI** is a suite of applications that integrates Workspace for Education functionality into third-party learning management systems ("LMS"). It includes:

i. **Google Assignments**, a tool allowing "End Users"[12] to distribute, collect, and grade student work.

ii. **Google Originality Reports**, a tool for automatically scanning a student's submitted assignment against a database of online content to detect potential plagiarism.

iii. **Google Drive LTI**, a tool allowing End Users to embed and share Drive files directly within their LMS.

[12] Google's various terms and disclosures do not define "End User." Google's Gemini defines "End User" as used by Google to mean "individuals who are authorized to use the Services and are managed by an Administrator," though Gemini confirms that it "cannot provide the exact terms of service documents "as it's a lengthy legal document and can be subject to changes." Gemini further notes "that the specific definition of "End User" can vary depending on the context and specific Google service that's being used."

iv. **Google Meet LTI**, a tool allowing End Users to establish secure meeting spaces to facilitate online learning within their LMS.

v. **Chrome Sync**, a feature allowing End Users to synchronize bookmarks, history, passwords, and other settings across all devices where they are signed into Chrome.

52. Core Services are available for students and administrators by default in every edition of Workspace for Education, including the free Fundamentals edition.

53. Other products and features are available at additional cost, such as the Google Admin security center and threat prevention, app-access control, and geographic data-limitation controls.

2. Google's Products generate and collect vast troves of children's data.

54. Workspace for Education Core Services and the Chrome browser are designed to collect substantial student data.

55. Google admits that these products collect significant information about school-aged children while they use Chromebooks, which includes "anything submitted, stored, sent, or received through core services by you or your school."

56. According to Google's own terms and policies, while children are using Core Services, Google collects at least the following information about them:

a. Children's account information, including "things like":

i. A child's name and

ii. A child's email address.

b. Children's activity while using the Core Services, including "things like":

i. The content a child has viewed;

ii. The content with which a child has interacted;

iii. Content a child creates, uploads, or receives from others, such as emails she writes and receives, photos and videos she saves, documents and spreadsheets she makes;

iv. People with whom a child has communicated;

v. People with whom a child has shared content; and

vi. "Other details" about a child's usage of the services.

c. A child's location information "as determined by various technologies such as IP address;"

d. Records of a child's communications with Google and its "partners" when a child provides feedback, asks questions, or seeks technical support; and

e. Technical information about a child:

i. A child's settings;

ii. The apps a child uses to access Google services;

iii. The browsers a child uses to access Google services;

iv. The devices a child uses to access Google services;

v. Browser type;

vi. Device type;

vii. Settings configuration;

viii. Unique identifiers;

ix. Operating system;

x. Mobile network connection;

xi. Application version number;

xii. Interaction of a child's apps with Google's services;

xiii. Interaction of a child's browsers with Google's services;

xiv. Interaction of a child's device with Google services;

xv. IP address;

xvi. Crash reports;

xvii. System activity; and

xviii. Data and time of a child's request.

57. In order to enhance its collection of student data, Google embeds hidden tracking technologies into its Core Services and Chrome OS.

58. One such technology is known as "browser fingerprinting," which allows Google to

create a unique identifier, or "fingerprint," of a child. That fingerprint is used to track a child's online activity across the internet as she navigates to different websites and web applications at the browser level. That means Google can use it to track a child even when she or her school administrator has disabled cookies or is using technologies designed to block third-party cookies, further reducing the ability to control and restrict the collection of their information. The profile created through fingerprinting transcends websites to identify a user and a user's online activities.

59. Many unique details and preferences can be exposed through a person's browser. The types of information Google is able to collect through this technology includes, but is not limited to, the following:

a. Browser attributes, such as:

i. Browser type, version, and extensions;

ii. Navigator properties;

iii. Presence of AdBlock;

iv. Cookies preferences;

v. Do Not Track preferences;

vi. Use of local storage;

vii. Use of session storage;

viii. User-agent;

ix. User-agent header (and other such headers, *e.g.*, Accept, Connection, Encoding, Language);

x. List of plug-ins;

xi. A picture rendered with the HTML Canvas element; and

xii. A picture rendered with WebGL.

b. Operating-system attributes, such as:

i. Operating system type and language;

ii. Time zone;

iii. Language and fonts;

iv. Keyboard layout; and

v. Screen resolution and color depth.

c. Hardware attributes, such as:

i. Battery level;

ii. CPU class;

iii. Device make;

iv. Device model; and

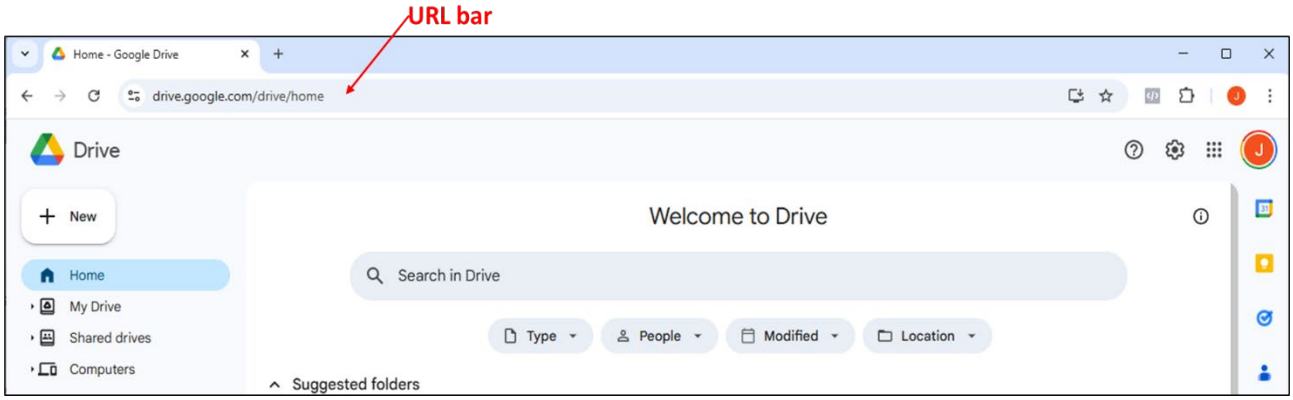
v. Device version.

60. Although these details may be generic, it is exceedingly rare that any two users will have identical data sets. This fingerprint thus enables Google and others to identify individual devices and thus individual children.

61. Google does not disclose that it employs this technology in its K-12 school-marketed products.

62. Google's use of browser fingerprinting is particularly significant given that students' access to the internet is not limited to the Core Services apps.

63. Because the Core Services run within the Chrome browser, they require a persistent internet connection to function and therefore also feature the Chrome browser uniform resource locator ("URL") bar, or address bar, during use. The URL bar is a text field in a web browser that displays the current web page's address, or URL. Users can enter text into the bar and navigate to different websites. For example, while a student is using the Google Drive app within Workspace for Education, she will see the address bar displayed at the top of the page:



64. By simply entering text into the URL bar, a child may freely navigate the open internet. And while she does, Google is tracking her every movement by using unique identifiers such as the browser fingerprint it has created about her while she used Core Services.

65. All Chromebooks also feature a persistent Chrome browser widget by default, which provides users access to the open internet:

66. That is because the Chrome browser is not an app; it is the fundamental interface of a Chromebook and Chrome OS.

67. Thus, while a child navigates the internet through the Chrome browser—which she may access either through the Chrome address bar or through the Chrome browser widget—Google generates and collects substantial personal information about her.

68. Because Google does not plainly disclose all the data it collects from children when they use its Products, Plaintiffs consulted Gemini, Google's "most capable and general [AI] model." According to Google, Gemini can "generalize and seamlessly understand, operate across, and combine different types of information[.]"[13] Google touts Gemini as providing users "the best the

[13] Alphabet Inc., 2023 Annual Report, at 4.

web has to offer" and meeting Google's "high bar for information quality."[14] Indeed, Google has integrated Gemini into features and products it markets to K-12 schools—including Chromebooks—promoting it as "a helpful tool to enhance and enrich teaching and learning experiences." According to one Google for Education executive, Google is "integrating Gemini capabilities like the Gemini app and NotebookLM into existing learning management systems, making it easier than ever for educators and students to teach and learn with AI."[15]

69. According to Google's Gemini, "Google collects a wide range of data when a user utilizes the Chrome browser." In addition to the data collected from children while they use the Core Services, some of the additional information Google collects while a child navigates the internet using the Chrome browser includes the following:

a. Browsing history:

i. URLs of websites visited;

ii. Timestamps of visits;

iii. Pages viewed within websites; and

iv. Duration of visits.

b. Search queries:

i. Search terms entered into the Chrome address bar;

ii. Search terms entered into the Google Search engine;

iii. Search suggestions; and

iv. Search auto-complete data.

c. Website interactions:

i. Links, buttons, and other interactive elements within websites and Chrome OS

[14] CNBC, *Google I/O 2024: Full Transcript of Sundar Pichai's Speech* (May 16, 2024), https://www.cnbctv18.com/technology/google-i-o-2024-full-transcript-of-sundar-pichais-speech-19413090.htm (last accessed April 4, 2025).

[15] Kitty Wheeler, *How Google's AI Tools are Revolutionising Education Tech*, TECHNOLOGY MAGAZINE (Jan. 27, 2025), https://technologymagazine.com/articles/how-googles-ai-tools-are-revolutionising-education-tech (last accessed April 4, 2025).

on which a child clicks;

ii. Whether the child returns to the search engine results page ("SERP") and how quickly;

iii. How long a child hovers over SERP results;

iv. A child's scrolling patterns on the SERP; and

v. Form submissions.

d. Cookies and site data:

i. Cookies stored by websites;

ii. Website data stored in local storage; and

iii. Cache data.

e. Download data:

i. Files downloaded from websites and

ii. Metadata about downloads.

f. Metadata about network traffic

g. Security data:

i. Data related to security events and

ii. Safe browsing data.

70. Google defines "personal information" as "information which you provide to us such as your name, email address, or billing information, or other data which can be reasonably linked to such information by Google, such as information with your Google account."[16]

71. Similarly, California law defines personal information as that which "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including "[g]eolocation data" as well as "Internet Protocol addresses" or "unique personal identifiers [or] online identifiers."[17]

[16] *Rodriguez v. Google LLC*, No. 20-cv-04688, 2022 WL 214552, at *5 (N.D. Cal. Jan. 7, 2025)

[17] *Id*. (citing Cal. Civ. Code § 1798.140).

72. In fact, Google has stated that "online information, such as IP addresses, routing and transmission information, session data, and more," when collected, "would paint an incredibly intimate picture of an individual's life."[18] Google has explained that

> a person's browsing history, email metadata, location information, and the exact date and time a person signs in or out of a particular online account . . . could reveal details about a person's political affiliation, medical conditions, religion, substance abuse history, sexual orientation, and . . . even his or her movements throughout the day.[19]

73. Google has warned about "[t]he civil liberties and human rights concerns associated with" access to such "sensitive" information.[20]

74. Further, students may and, upon information and belief, do access Core Services and the Chrome browser using family-owned devices, enabling Google's tracking technologies to harvest data about those devices and users of those devices—such as students' household members—as well. One result is that the data purportedly collected about and attributed to a child may actually belong to a family member, skewing the profile that is built about that child in ways that may further harm the child. And because its platforms are accessible anywhere, Google may track children wherever they go, including in their own homes.

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

76. The Stolen Information far exceeds what could be legally or traditionally characterized as "education records."

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

78. The Stolen Information, when combined and processed, enables Google to build

[18] ACLU, *ECTR Coalition Letter* (June 6, 2016), https://www.aclu.org/documents/ectr-coalition-letter (last accessed April 4, 2025).

[19] *Id.*

[20] *Id.*

dynamic, intimate dossiers of children.

79. As Google's Gemini observes, the above information provides robust insight about a child's identity, behavior, interests, habits, and preferences.

80. User-data generation and collection is an intentional design choice.

81. As one court recently observed, "Early on, Google understood that the information gleaned from user queries and click activity were a strong proxy for users' intent and that such information could be used to deliver superior results."[21]

82. The court also noted that "the degree of privacy a [general search engine] offers reflects a series of individual design decisions. Whether to track a user's sessions data is one such decision."[22] But such data is not necessary for a general search engine to function. Other search engines fully anonymize user click data and do not track user sessions.

83. The court further identified other design choices that reflect a search engine's measure of privacy, such as how user data is used and how long it is retained.[23]

84. Google could design its Core Services and Chrome browser, which it markets and sells to K-12 education institutions for use by children, to minimize the amount of data it collects from students, but instead it optimizes those Products for data extraction.

85. Gemini admits that it would be "possible for Google to design Google Workspace for Education to further reduce data collection." It explains that Google "setting a default privacy mode that limits data sharing and tracking could reduce the amount of data collected by default." It also suggests that "[e]mploying differential privacy techniques could mask individual user data while preserving statistical trends." It further provides that "[v]isualizing data flows and processing steps could increase transparency and accountability," and suggests that "[c]onducting regular privacy impact assessments could identify potential risks and opportunities for improvement."

[21] Mem. Op., *United States et al. v. Google LLC*, 20-cv-3010 (APM), ECF No. 1032, at 276 ("Mem. Op.").

[22] *Id*. at 44.

[23] *Id*. at 44–45.

86. That Workspace for Education Core Services and the Chrome browser are not designed to optimize privacy is an intentional, self-interested choice by Google to prioritize profit over children's privacy, safety, health, and wellness.

87. Google does not limit a child's access to the internet through the Chrome browser by default, which facilitates the generation and collection of data from children as they navigate the internet through the Chrome browser. Through this design choice, Google externalizes the burden of protecting student privacy to the public.

88. For example, Google states that "[t]he [education institution] customer should understand requirements around limits on collection and processing of Customer Personal Data (*e.g.*, that the collection and processing should be limited to what is needed for the specific purpose)."

89. Further, Gemini suggests that schools "can provide training to students and staff on data privacy and best practices, encouraging them to be mindful of their online activities and data sharing." Gemini falsely states that "Google provides clear information about data collection and usage practices in Google Workspace for Education, empowering users to make informed choices." But there is nothing clear about Google's collection and usage practices, other than that such practices are undertaken without the consent of students or their parents.

90. The result is that, through Workspace for Education's Core Services and the Chrome browser, Google generates and gains access to far-reaching personal information of students.

91. The Stolen Information, including data about children under 13 years of age, far exceeds that which is reasonably necessary for children to participate in any school activity that is facilitated by Google's Products in violation of Children's Online Privacy Protection Act ("COPPA"), the federal statute that governs the collection of children's data by operators of online services. *See* 15 U.S.C. § 6502; 16 C.F.R. § 312.7.

B. Google's disclosures regarding its data practices are incomprehensible.

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

93. Google is required to provide disclosures regarding its data practices so that a

reasonable user would understand them and know what they were consenting to.

94. Further, before collecting personal information from children under 13 years of age, Google is required to provide parents notice of its data practices that is "clearly and understandably written, complete," and contains "no unrelated, confusing, or contradictory materials." *See* 15 U.S.C. § 6502; 16 C.F.R. § 312.4.

95. Google provides certain disclosures, but these disclosures are factually and legally inadequate to enable users to understand them and know what they are consenting to. A reasonable person cannot understand Google's data practices—especially as they pertain to students in the K-12 setting—by reviewing Google's disclosures.

96. Google does not provide parents of students under 13 years of age notice of its data practices that is clearly and understandably written, complete, and contains no unrelated, confusing, or contradictory materials.

97. In fact, a reasonable person may not even be able to definitively determine which disclosures govern students' use of its Products. Such information is dispersed across multiple policies, terms, agreements, and FAQs, all found on a host of webpages, many of which cross-reference and/or incorporate each other. For example, relevant information appears in at least the following places:

a. Google Workspace for Education Terms of Service;

b. Google Workspace for Education Privacy Notice;

c. Google Workspace for Education Service Data Addendum;

d. Google Cloud Privacy Notice;

e. Google Cloud Data Processing Addendum (Customers);

f. "Order Form," which is undefined and unavailable but controls over other provisions;

g. Google Workspace Services Summary;

h. Google Workspace Service Specific Terms;

i. Google Workspace, Additional Product Terms;

j. Google Workspace Admin Help, "Service categories available to Google Workspace for Education Users";

k. Google Workspace Admin Help, "Communicating with Parents and Guardians about Google Workspace for Education;

l. Google Workspace Admin Help Center, "Google Workspace for Education Overview";

m. Google Cloud Identity – Services Summary;

n. Google Privacy & Terms, "Privacy Policy";

o. Google Privacy & Terms, "Terms of Service";

p. Google Privacy & Terms, "Technologies";

q. Google Privacy & Terms, "FAQ";

r. Google Safety Center, "Content safety";

s. Google for Education, Privacy and Security;

t. Google for Education, Products;[24] and

u. Google for Education, Privacy and Security FAQ.

98. Google also cites agreements with "customers," such as schools and school districts, in reference to material terms—such as collection and use of student information permitted by customer consent—which are not available to parents.

99. The terms and policies that appear to apply only to Workspace for Education Core Services (but that do not constitute all terms and policies governing Workspace for Education) alone constitute tens of thousands of words and include dozens of hyperlinks to other voluminous webpages.

100. While the sheer number of links to relevant information make it falsely appear as if Google's disclosures are sufficient, even if a student or her parent reads every single word of this information, it is not possible to determine what Google is actually doing in practice. As a result,

[24] This page states that Gemini for Google Workspace "is covered under the Google Workspace for Education Terms of Service," but those Terms do not mention Gemini.

there has been no meaningful disclosure by Google of its data mining and monetization policies.

101. Much of this information contains vague, incomplete, or conflicting language regarding Google's data practices.

102. It is thus impossible for a parent or any other person to reasonably understand the extent of Google's generation, collection, aggregation, use, and sharing of personal information belonging to school-aged children.

103. Google's disclosures thus fail to meet general data-privacy standards, as well as the heightened requirements of COPPA. *See* 15 U.S.C. § 6502; 16 C.F.R. § 312.4.

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

104. Google fails to obtain informed, ongoing consent for its sweeping collection and use of student data, including personal and private information. Specifically, Google fails to: (1) provide users adequate information to support informed consent; (2) obtain consent from a person with authority to grant it; (3) determine whether students' use of its products is voluntary; and (4) provide students proper consideration in exchange for their agreement to its data practices.

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

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

105. As discussed in section II.B., *supra*, Google does not make informed user consent possible because it does not provide users the information regarding its data practices necessary to support informed consent.

106. Google fails to provide an explanation that may be reasonably understood and that discloses (1) the data or categories of data it collects on users; (2) the ways in which it will use such data; and (3) the entities that will have access to such data.

107. Google also fails to provide parents the detailed notice expressly required by COPPA. *See* 16 C.F.R. § 312.4.

108. Further, even if schools were authorized to act as agents for parents in consenting to Google's data practices, Google does not provide schools adequate information about those practices

to support informed consent. Its "[n]otice template for schools when gathering parent or guardian consent" does not fully reflect the practices set out in Google's many terms and policies, including the types of data collected, how data is used, and with whom data is shared, or even a comprehensive list of applications available to students through Workspace for Education.

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

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

110. One of the privacy policies that governs Workspace for Education directs parents to discuss any issues with their school—"if you have questions regarding the management of Google Workspace for Education accounts or the use of information by your child's school"—though it does not provide a method for parents to obtain information generated, collected, and used by Google.

111. Accordingly, when Plaintiff Dunbar requested access to her child's data, Google denied her request. Google informed her that, because her child was using an account "created and managed by a school for use by students and educators," she would need to "contact her admin to: access your personal information, limit access to features or services, delete personal information in services or delete your entire account" as provided in its Google Workspace for Education Privacy Notice, to which it linked.

112. When Plaintiff Gridley requested access to her children's data, Google also instructed her to "contact your admin to: access your personal information, limit access to features or services, delete personal information in services or delete your entire account."

113. Similarly, when Plaintiff Schwarz requested access to his child's data, Google informed him that "[s]chools are responsible for managing student data and providing parents with access to that data . . . . Therefore, we recommend that you contact your student's school directly to

request access to their data."

114. Google's refusal to hand over this information is a direct and knowing violation of COPPA, which requires that operators of websites or online services to provide parents access to all personal information they have collected from children under 13. *See* 15 U.S.C. § 6502; 16 C.F.R. § 312.6.

115. Further, Google represents that school administrators can help parents "access your personal information" and "delete personal information in services or delete your entire account." It further states that, "for Google Workspace for Education accounts, all user data is owned and managed by the organization, not Google." Google states that "[t]he customer should understand requirements around the rights of individuals related to the processing of their Customer Personal Data," including "access, correction, erasure, and export."

116. However, schools do not possess all necessary information about Google's data practices, nor do they possess, retain, control, or even have access to all the student data collected, stored, processed, and used by Google.

117. Plaintiff Dunbar's school district, for example, was unable to access all of H.D.'s personal information generated and obtained by Google during her use of her school-issued Chromebook.

118. According to the school district, Google provides no way to grant a parent access to individual student data without granting access to all district data in violation of various state and federal confidentiality laws. Thus, Plaintiff Dunbar still does not know what personal information Google has generated and taken from her child through its school-marketed Products.

119. Plaintiff Schwarz's school district was able to provide him access to certain data collected from his child, though the data set provided was: (1) in a format that was largely inaccessible or undecipherable and (2) plainly incomplete. Despite his best efforts, he was unable to decipher much of the data he was able to access.

120. Moreover, some of the personal information that Plaintiff Schwarz was able to access was more than five years old, and certain data were set to be retained "forever."

121. Students and parents thus have no way to control—correct, delete, or otherwise modify—their personal information that is generated, taken, and used by Google.

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

123. Plaintiffs do not have a reasonable understanding of Google's data practices.

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

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

125. Before collecting and using children's personal and private information, Google fails to obtain effective consent.

126. As detailed herein, Google generates and collects data directly from school-aged children—including personal and personally identifiable information—through their use of Workspace for Education Core Services and the Chrome browser.

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

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

129. Further, COPPA contains a heightened parental consent requirement that Google must meet before it may collect personal information from children under 13. *See* 16 C.F.R. § 312.5. Specifically, it requires that Google "obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented." *Id.* § 312.5(a)(1). Google does not meet any of the exceptions to this consent requirement. *Id.* § 312.5(c).

130. Google does not obtain consent from minors' parents for its collection or use of minors' data as described herein, under generally applicable standards *or* the heightened COPPA standards that protect children under 13.

131. Google instead purports to unilaterally absolve itself of this duty and shift the burden to schools to obtain the necessary consent for Google's collection and use of student data, without obtaining any manifestation of assent from parents themselves. The Google Workspace for Education Terms of Service state that "Customer [education institution] is responsible for any consents and notices required to permit" Google to collect and use students' personal information, including as required under COPPA.

132. Indeed, Google states that it "does not provide support for gaining and recording user consent for all of your activities."

133. At no time does Google require any evidence that parents have agreed to schools acting on their behalf for the purposes of consenting to Google's data practices or that schools actually have obtained consent from parents.

134. Schools do not own the data that Google generates about and extracts directly from students.

135. School administrators are not legal guardians of students.

136. Students own their own personal and private information.

137. Schools cannot legally consent—in lieu of parents or over parents' objections—to the direct generation, collection, or use of personal information about and belonging to children by a third party, particularly a privately owned, for-profit technology company for commercial purposes, even if such collection and use may confer a benefit to schools that is administrative, pedagogical, or otherwise.

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

139. Students retain significant privacy interests in their personal information contained within education records.

140. Google admits that it enables school administrators to prevent parents from accessing their children's data. It states that "[i]f you have a school account, your [school] can choose to download your data and to limit you from downloading it."

141. Google incorrectly states that it is the responsibility of schools to ensure compliance with COPPA, including its notice-and-consent requirements.

142. Further, schools do not obtain parental consent to Google's collection and use of student data as a parent's agent or intermediary, because schools lack the information necessary to support informed consent, as detailed herein. Google thus generates, takes, uses, and discloses children's personal information without obtaining effective consent before doing so or anytime thereafter.

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

143. Google additionally or alternatively states that it need not obtain parental consent to collect and use student data under the Family Educational Rights and Privacy Act ("FERPA").

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

145. In its Workspace for Education Terms of Service, Google states that "to the extent that Customer Data includes FERPA Records, Google will be considered a 'School Official' (as that term is used in FERPA and its implementing regulations) and will comply with FERPA." But FERPA governs federally funded schools, not private companies. Nothing in FERPA exempts private companies from their legal obligations, especially those they owe to children and their parents.

146. Further, Google does not obtain and use student data as contemplated by the school-official exception of FERPA.

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

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

149. Google generates and collects personal information in excess of student education

records as defined by FERPA.

150. Google generates, collects, and uses data in excess of legitimate educational interests as contemplated by FERPA. Google rediscloses personal information to a host of third parties without prior parental consent.

151. FERPA thus does not absolve Google of its duty to obtain parental consent before generating, obtaining, using, and disclosing children's personal and private information.

D. Google makes no effort to determine whether students' use of its Products is voluntary as is necessary to support consent.

152. Voluntariness is an essential element of contract formation.

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

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

155. Schools use Google's Products to support a host of pedagogical and administrative functions.

156. Plaintiffs were not given a choice to forgo using Google's Products.

157. Students are not able to opt out of using Google's Products as part of their education.

158. Even if students theoretically could opt out of using Google's Products, Google may not place students and their parents in the position of having to choose between their rights to privacy and their right to an education, or risk compromising their relationship with school personnel in order to protect their rights. Such inherently coercive circumstances do not support voluntary consent.

159. Indeed, Google itself understands and intends this unfair choice: in the "Notice template for schools when gathering parent or guardian consent" Google provides on its website (which it neither requires nor confirms has been performed), Google advises that schools "may wish to describe . . . how not providing consent to use Google services will impact the educational experience. For example, students who cannot use Google services may need to use other software to complete assignments or collaborate with peers." Consent obtained through such coercion is not voluntary, particularly given that many schools lack the resources to provide alternative, privacy-

protective software to facilitate a child's choice to opt out.

160. As Gemini states, this arrangement "can indeed place parents in a position where they feel they must choose between their child's right to privacy and their access to a full education."

161. Because students lack the ability to decline or avoid using Workspace for Education and the Chrome browser, any purported agreement by them to Google's terms and policies is unenforceable.

E. Google does not provide students sufficient consideration as necessary to support any agreement to be subjected to Google's data practices.

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

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

164. Every state in the United States has laws guaranteeing children the right to an education.

165. That right includes the right for students to avail themselves of products and services offered by their school, especially those that are necessary to participate in and receive an education.

166. Schools use Google's Products to support a host of pedagogical and administrative functions.

167. Students' use of Google's Products is thus a part of the education to which they are already legally entitled.

168. Google does not offer parents or students any additional benefit in excess of those to which students are already entitled that might constitute sufficient consideration to support any agreement to Google's terms and policies, including those governing Google's data practices.

169. Plaintiffs and Class members were provided no additional consideration that might have supported any agreement to Google's data practices.

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

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

IV. Google uses the personal information it generates and collects from students without effective consent for commercial purposes.

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

172. Like most surveillance-technology companies, Google does not collect user data for the primary purpose of providing the raw data itself to third parties, nor for the limited purpose of assisting families with their children's educational pursuits. Instead, Google collects, combines, and analyzes children's data for the purpose of developing, improving, maintaining, and disseminating its own digital, data-derived products for considerable profit.

173. Google collects student data (which Google misleadingly describes as "customer data" or "service data") for commercial purposes, including research, development, evaluation, and improvement of its services, and to make recommendations.

174. Gemini explains that Google benefits financially from data collected from Workspace for Education in a variety of ways. For example, according to Gemini, Google uses student data for product improvement and for "making [its products] more attractive to both educational institutions and businesses," which "can lead to increased adoption and revenue from premium subscriptions."

175. Gemini further states that Google can use student data "to train Google's AI and machine learning models, which can then be applied to other products and services that generate revenue."

176. Google also uses the Stolen Information to facilitate future product development. As Gemini explains, "[a]nalyzing user behavior and preferences can help Google identify new opportunities for product development, potentially leading to new revenue streams."

177. Although Google markets these Products as conferring to schools and school districts administrative and pedagogical benefits, they are undeniably commercial, for-profit products that have helped Google build a multitrillion-dollar surveillance-technology empire.

178. To power its massive and growing suite of data-derivative products and provide its

customers access to granular student analytics, Google compiles the data it collects through each of its platforms and uses it to build, improve, and market its suite of products. The Workspace for Education Core Services now includes dozens of products, as described in Section II.A., *supra*.

179. These products exist only through Google's sweeping generation, collection, retention, disclosure, and use of personal and private information that it has unlawfully obtained from students in the context of compulsory K-12 education.

180. These products also enable Google to continue generating and collecting vast troves of student information.

181. Google also uses student data to generate student "analytics," which it markets for use by school personnel.

182. Such analytics purport to provide customers "insights" into student engagement, progress, and performance. The types of personal information customers can access include at least the following:

a. Student engagement, including:
    i. Assignment submission rates;
    ii. Student participation in discussions;
    iii. The amount of time that a student spends on specific assignments;
    iv. Student login activity; and
    v. Information related to students viewing posted materials.

b. Student progress and performance, including:
    i. Student grades and scores on assignments and quizzes;
    ii. Assignment completion status;
    iii. Individual student progress;
    iv. Trends in student performance; and
    v. Detailed results from quizzes and other student responses.

c. Content usage, including:

i. How students interact with different types of content.

d. Communication and interaction metrics, including:

i. Data related to how a student communicates within Google Classroom and

ii. Data related to how a student responds to feedback.

183. Google also facilitates "personalized" learning through its generation, collection, and use this data.

184. Student data collected through Google's Core Services and Chrome browser is combined to enhance its suite of products to facilitate deeper and more individualized analytics.

185. If Google is unable or unwilling to provide services that do not require vast troves of personal and private user information to function, it should not be marketing those products for use in K-12 environments in which attendance is compulsory and the users are children.

2. Google shares student data with third parties for commercial purposes.

186. Google states that it shares personal information to "our affiliates," which it defines as "the Google group of companies," and "other trusted businesses or persons to process it for us," which it does not define nor comprehensively identify. Data processing by or on behalf of Google may include acts that:

a. help operate its data centers;

b. deliver its products and services;

c. improve its services;

d. measure the performance of its products and services;

e. develop new services;

f. improve its internal business processes;

g. communicate with users; and

h. offer additional support to customers and users.

187. Google also shares user data with third parties when Google believes that disclosure of the information is "reasonably necessary" to:

a. respond to any applicable law, regulation, legal process, or enforceable governmental request;

b. enforce its own terms of service;

c. address fraud issues;

d. address security issues;

e. address technical issues; or

f. protect Google from harm to its own rights, property, or safety.

188. Google also shares user data in the event of a merger, acquisition, or sale of its assets.

189. Google also partners with numerous companies in the generation, collecting, analysis, use, and/or sharing of student data.

190. Google maintains a robust, open Application Programming Interface ("API") program.

191. Companies with access to Google's API gain access to significant amounts of personal and private information about and belonging to school-aged children in real time.

192. Such information includes, but is not limited to, a student's full name, courses, coursework, submissions, classroom-assigned unique identifier, when coursework is begun, whether coursework is submitted late, individual grades, grade history, responses, guardian information, and associated metadata.

193. Google admits that it has partnered with more than 20 EdTech companies for purposes of data sharing, including Kahoot!, Pear Deck, IXL, ReadWorks, and Nearpod.

194. In fact, Google's API is configured to connect with thousands of platforms.

195. Google's primary value to third-party partners depends on maximizing access to student data.

196. Data exchanged through these partnerships—including children's personal and private information—enables Google and participating partners to develop, improve, expand, deliver,

support, market, and sell their products and services.

197. Although Google admits to using user data in certain ways that could be lawful if that data was lawfully obtained, those uses are unlawful because Google obtains the data it generates and collects from students through Core Services and the Chrome browser without effective consent. In other words, because the Stolen Information is stolen, there are no legitimate uses of it.

3. Google retains student data for an unreasonable amount of time.

198. Google also retains Stolen Information of children under 13 longer than is reasonably necessary to fulfill the purpose for which it purportedly collects the information.

199. Google retains some of this information indefinitely.

200. In so doing, Google violates retention regulatory requirements of COPPA, which require that "[a]n operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." 16 C.F.R. § 312.10.

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

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

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

202. On its Classroom Help webpage, Google falsely states that it "respects your privacy." Google does not respect users' privacy, as evidenced by its invasive and surreptitious data practices described herein.

203. On its Security and Privacy webpage, Google falsely states that it "strictly uphold[s] responsible data practices so every product we build is private by design." Google does not build its products to be private by design but instead designs them to maximize the generation and collection of user data—including the Stolen Information described herein—as its business model requires.

204. On that same webpage, Google falsely states that it "create[s] easy to use privacy and security settings so you're in control." Any such purported settings are not easy to use and do not

provide students or parents any real measure of control over their personal information.

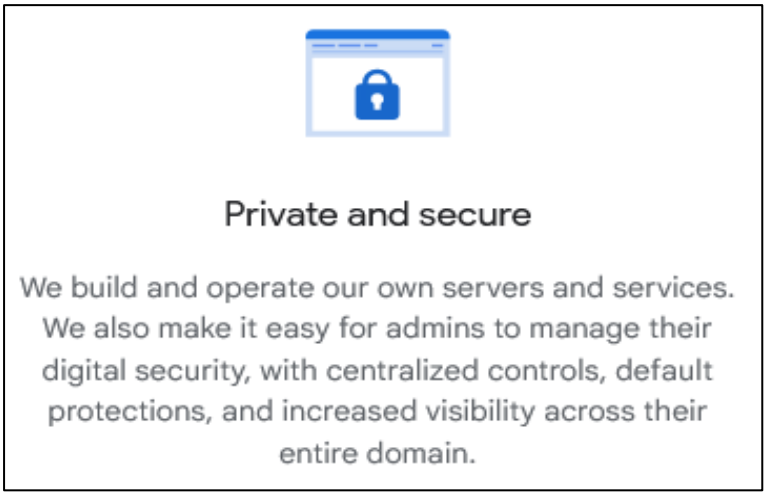
205. Google repeatedly and misleadingly conflates the technical, practical, and legal concepts of data privacy and data security across its website. Data privacy and data security have different meanings in every relevant sense.

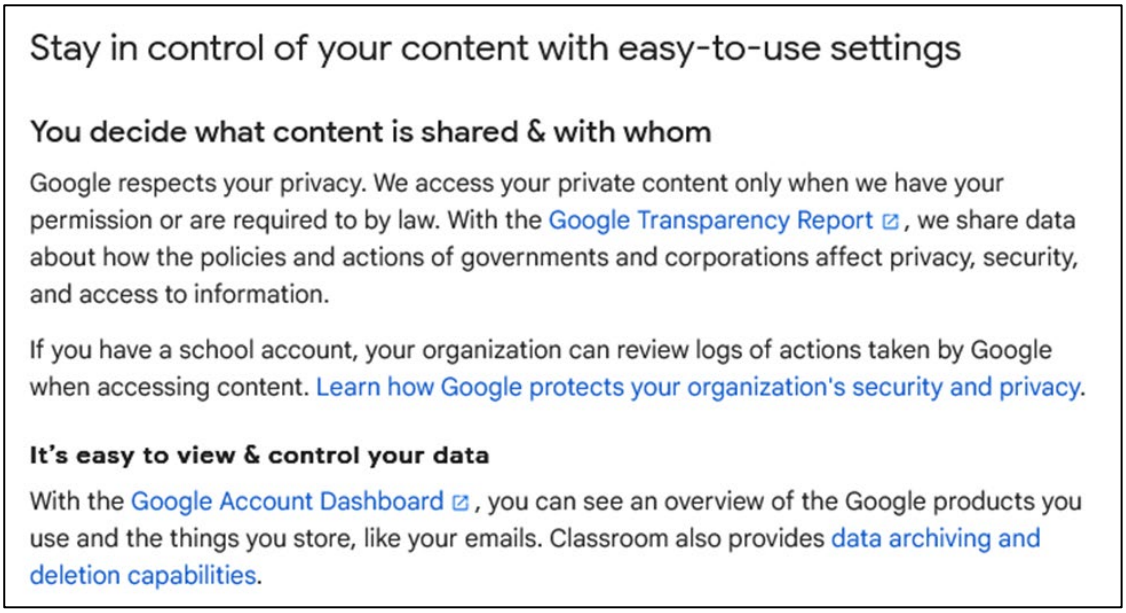
206. On its Google for Education, Privacy and Security "Our values" webpage, Google falsely states" that "[p]rotecting your privacy starts with the world's most advanced security." Under the law, protecting privacy starts with companies not generating and collecting individuals' data in the first place.

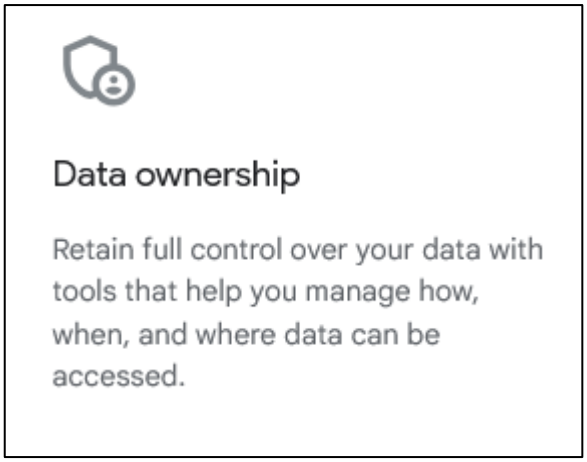
207. In its Google for Education "Guardian's Guide to Privacy and Security," Google falsely states that, "[w]ith Chromebooks and Google Workspace for Education, privacy is not a feature, it's a priority." Privacy is neither a feature nor a priority in Google's Products, which are designed and built to generate and take students' data.

208. In that same guide, Google falsely states that "[p]rivacy is at the very foundation of our educational platform." The foundation of Google's Products is taking and monetizing user data.

209. Google highlights its purported commitment to privacy throughout its website:







210. These statements are undermined by the design of Google's Products and its business model.

B. Google falsely states that student data belongs to schools and not students.

211. On its Privacy and Security "Our values" webpage, Google falsely states that schools retain complete control of data collected through Workspace for Education accounts. Schools do not retain control of the data that Google generates about and collects from students and their parents through Workspace for Education, Google does.

212. In its Workspace for Education Service Data Addendum, Google misleadingly refers to personal and private information about and belonging to students that is generated and extracted

by Google as "Customer Data" that belongs to and/or is provided by schools.

C. Google falsely states that it is FERPA compliant.

213. Google falsely and repeatedly states that its services may be used by schools in compliance with FERPA throughout its website. In its Workspace for Education Terms of Service, for example, Google states that "to the extent that Customer Data includes FERPA Records, Google will be considered a 'School Official' (as that term is used in FERPA and its implementing regulations) and will comply with FERPA." But Google does not obtain and use student data as contemplated by the school-official exception of FERPA, thus its conduct does not fall within this exception.

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

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

216. Google generates and collects personal information in excess of "education records" as defined by FERPA.

217. Google generates, collects, and uses data in excess of legitimate educational interests as contemplated by FERPA. Google rediscloses personal information to a host of third parties without prior parental consent.

D. Google falsely states that it is COPPA compliant.

218. Google falsely states that it complies with COPPA. In fact, Google violates numerous provisions of COPPA.

219. Google fails to provide parents complete, understandable notice of its data practices.

220. Google fails to obtain parental consent before taking and using children's personal information.

221. Google falsely informs schools that they are authorized to consent to the taking and using of children's data under COPPA.

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

223. Google retains children's personal information for longer than is necessary to fulfill the stated purposed for which the information was collected.

224. Google fails to provide parents access to the personal information it has collected from their children.

E. Google falsely states that it complies with the Student Privacy Pledge.

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

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

b. "We will not sell student PII."

c. "We will not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students."

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

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

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

g. "We will incorporate privacy and security when developing or improving our educational products, tools, and services and comply with applicable laws."[25]

226. Google does not adhere to any of these commitments, as described herein.

F. Google intends that the public rely on its misrepresentations.

227. Google intends that the public—including school personnel and parents—rely on these false and misleading representations in determining whether and how to use its products.

228. Parents rely on these misrepresentations directly themselves or indirectly through

[25] Student Privacy Pledge, K-12 School Service Provider Pledge to Safeguard Student Privacy 2020, https://studentprivacypledge.org/privacy-pledge-2-0/ (last accessed April 4, 2025).

trusted school personnel who rely on these misrepresentations in deciding to utilize Workspace for Education. If school personnel had not been deceived as to Google's data practices, they would not have subjected students to those practices. Schools' use of Workspace for Education and the Chrome browser thus permits an inference that they relied on Google's material, false representations about Google's data practices.

229. Further, these false and misleading statements were likely to mislead and deceive the public and harm the public interest. The public has an interest in protecting children from Google's exploitative data practices, especially while attending school and engaging in school activities, such as completing assignments.

V. Google's nonconsensual data practices harm children.

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

231. Google's policies and practices irreparably damage school-aged children by violating their privacy and their right to control their own personal information.

232. Google's policies and practices also harm school-aged children in the form of diminution of the value of their private and personal data and content.

233. The inability to control their own data and Google's collection and use thereof further impedes students' ability to control what is done with it after it is taken by Google.

234. Parents are entitled to be fully informed of the potential benefits and risks that Google's data practices pose to all stakeholders, especially children. Once fully informed, it is up to parents to decide whether to subject their children to those risks in exchange for valuable consideration beyond the education services to which they are already entitled.

235. These harms are actual and concrete and not merely hypothetical. Google steals children's personal and private information, which it monetizes at the expense of children's privacy, property, and wellbeing.

A. Google harms children by invading their privacy.

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

harm.

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

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

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

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

241. Google's tracking occurs no matter how sensitive or personal a child's online activities are, as Google's data practices are indiscriminate and sweeping.

242. By correlating individuals' online activities—such as their browsing history—with other personal information, Google collects additional data to add to its intimate profile of those individuals without valid consent.

243. Further, Google provides children inadequate access to and control over their personal information.

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

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

Constitution itself."[26]

246. Google itself has acknowledged that privacy is a human right and that violations of privacy are violations of human rights.

247. Google has also publicly declared that non-consensual electronic surveillance is "dishonest" behavior. It has agreed that obtaining sensitive information about Americans' online activities without court oversight was an unacceptable privacy harm because it "would paint an incredibly intimate picture of an individual's life" if it included "browsing history, email metadata, location information, and the exact date and time a person signs in or out of a particular online account."[27]

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

249. Google's creation, collection, use, and disclosure of personal information about and belonging to students and their parents is highly offensive by any standard.

B. Google harms children by persistently surveilling them.

250. Google harms children by persistently surveilling, monitoring, and tracking them while they use its Products.

251. Research has shown that persistent surveillance decreases opportunities for children to exercise autonomy and independence. Persistent surveillance hinders children's development of self-regulation and decision-making that are crucial to aspects of responsibility and self-identity.[28] Continuous surveillance can also increase passivity and self-censorship in children rather than genuine expression, compromising their rights to freedom of thought, conscience, communication,

---

[26] Noah Joshua Phillips, *Taking Care: The American Approach to Protecting Children's Privacy*, U.S. FEDERAL TRADE COMMISSION (Nov. 15, 2018), https://www.ftc.gov/system/files/documents/public_statements/1422695/phillips_-_taking_care_11-15-18_0.pdf (last accessed April 4, 2025).

[27] ACLU, *ECTR Coalition Letter* (June 6, 2016), https://www.aclu.org/documents/ectr-coalition-letter (last accessed April 4, 2025).

[28] Caroline Stockman and Emma Nottingham, *Surveillance Capitalism in Schools: What's the Problem?*, DIGITAL CULTURE & EDUCATION (2022) at 6.

creativity, and speech.[29] It emphasizes compliance with the current social order instead of the cultivation of identity and dignity.[30]

252. Persistent surveillance at school normalizes surveillance in other areas of life, and trains children not to value their own and others' privacy and autonomy.[31] It also normalizes the exploitation of children, their personal information, and their educational development for third-party commercial gain without knowledge, consent, or compensation.[32]

253. The oppressive potential of Google's surveillance practices is proportional to the invisibility and pervasiveness of those practices.[33]

254. Google constantly surveils children. Google subjects children to numerous tracking technologies that allow it to track a child across the web in perpetuity.

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

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

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

257. Schools and school districts have been particularly and increasingly targeted by cybercriminals in recent years, which has resulted in leaks of highly personal and sensitive information about children, some of which perpetrators have made publicly available.

258. Indeed, another major student information system was hacked in December 2024, compromising the personal and private information of tens of millions of students dating back

[29] *Id*.

[30] *Id*.

[31] *Id*. at 6.

[32] *Id*. at 7.

[33] *Id*. at 3.

decades.[34]

259. Exposures like these can have immediate and long-term consequences for children. As explained by one cybersecurity professional, whose son's school was hacked, "It's your future. It's getting into college, getting a job. It's everything."[35]

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

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

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

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

263. As described herein, Google uses Stolen Information to create products that purport to analyze and predict student performance and behavior.

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

---

[34] Zack Whittaker, *Malware Stole Internal PowerSchool Passwords From Engineer's Hacked Computer*, TECHCRUNCH (Jan. 17, 2025), https://techcrunch.com/2025/01/17/malware-stole-internal-powerschool-passwords-from-engineers-hacked-computer/ (last accessed April 4, 2025).

[35] Natasha Singer, *A Cyberattack Illuminates the Shaky State of Student Privacy*, THE NEW YORK TIMES (July 31, 2022), https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html (last accessed April 4, 2025).

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

266. Google's models define their own metrics, which Google uses to justify their results, creating and perpetuating a pernicious and untested feedback loop.

267. The datafication of a child and their learning process, for commercial purposes, brings about a social disempowerment that negatively affects the child's education in the moment of learning and also, therefore, the future of a free and sustainable society.[36]

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

268. Beyond taking and using the Stolen Information for purposes of algorithmic profiling, Google denies children and their parents the ability to access and review the data it takes from them and understand how their data is used and who has access to it.

269. Further, the algorithmic models on which Google's Products are built are entirely opaque.

270. Families are thus unable to review the data collected and aggregated, the algorithmic models used to generate predictions, or the assumptions on which those models are based or otherwise understand how their data is processed, interpreted, and used.

271. As previously discussed, schools may rely on the Stolen Information and the data-derived products developed by Google to make decisions that affect children's lives now and in the future.

272. Google's practices harm families by denying them the ability to: (1) assert their rights by providing—or declining to provide—informed consent before their information is irreversibly compromised; (2) respond effectively to issues involving their personal information; or (3) make

[36] *See, e.g.*, Emma Nottingham, Caroline Stockman, Maria Burke, *Education in a Datafied World: Balancing Children's Rights and School's Responsibilities in the Age of COVID 19*, COMPUTER LAW & SECURITY REVIEW (July 2022), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8958095/pdf/main.pdf (last accessed April 4, 2025).

meaningful decisions regarding the collection, storage, and use of their information. Families are also unable to know and object to the predictions generated by unknown data and to how third parties use those predictions.

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

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

274. Personal data 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.

275. A robust market exists for user data, especially children's personal information. User data has been analogized to the "oil" of the digital economy.[37]

276. Google itself has paid users for the types of data it harvests from school-aged children.[38] As early as 2012, Google was offering users Amazon gift cards worth up to $25 to collect and use their data for research, marketing, and product development and improvement.[39] The value of Plaintiffs' data is worth far more than that of consenting adults more than a decade ago. In 2023, for example, one prominent education-technology vendor observed that, "[a]ccording the U.S. Department of Education, the value of a student records on the black market is $250 to $350."[40] Such

[37] *The World's Most Valuable Resource is No Longer Oil, But Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last accessed April 4, 2025).

[38] Jack Marshall, *Google Pays Users for Browsing Data*, DIGIDAY (Feb. 10, 2012), https://digiday.com/media/google-pays-users-for-browsing-data/ (last accessed April 4, 2025).

[39] *Id*.

[40] *Student Data Privacy: Everything You Need to Know*, POWERSCHOOL (June 20, 2023), https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ (last accessed April 4, 2025).

information in legal markets would be even more valuable.

277. Furthermore, most U.S. consumers value their data and their privacy. Accordingly, an overwhelming majority engage in efforts to protect their data: 86 percent of U.S. consumers report caring about data privacy and wanting more control; 79 percent are willing to spend time and money to protect their data; and nearly half have terminated relationships with both online and traditional companies over data-privacy concerns, especially younger consumers.[41]

278. As one court recently observed, "Google recognizes that users increasingly care about the privacy of their online activity."[42]

279. The EdTech market is valued at nearly a quarter of a trillion dollars.[43] The broader market for data, especially for children's personal information, is larger still.

280. The Stolen Information at issue has significant economic value.[44]

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

282. Further, when students access Core Services and browse the internet using the Chrome browser, Google secretly embeds numerous persistent tracking mechanisms on their computers and

---

[41] Cisco, *Consumer Privacy Survey: Building Consumer Confidence Through Transparency and Control* at 5 (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (last accessed April 4, 2025).

[42] *United States v. Google LLC*, No. 20-cv-3010 (Aug. 5, 2024), Mem. Op. at 43.

[43] Louise Hooper, *et al*., *Problems with Data Governance in UK Schools*, Digital Futures Commission, 5Rights Foundation (2022), https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf (last accessed April 4, 2025).

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

web-browsers, which allow Google to track students' browsing histories and correlate them with the student, device, and browser identifications to identify and target the student.

283. These practices circumvent the efforts of students and school personnel to prevent others from accessing student data.

284. Google's actions have thus caused students economic injury.

285. By generating, collecting, using, and disclosing the Stolen Information, Google has diminished the value of that information and student's future property interest.

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

287. Google's actions caused damage to and loss of students' property and their right to control the dissemination and use of their personal and private information.

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

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

289. Recent research shows that nearly 80 percent of adults reported being very or somewhat concerned about how companies use data collected about adults,[45] and the number of those concerned about their online privacy is growing quickly.

290. Protective behaviors are on the rise, with 87 percent of adults in the U.S. using at least one privacy- or security-protecting tool online.[46]

291. An even greater percentage of parents value protecting their children's personal data, including their identity (90%), location (88%), health data (87%), age (85%), school records (85%),

[45] Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last accessed April 4, 2025).

[46] Stephanie Liu, *US Consumer Privacy Attitudes In 2022*, FORRESTER (Sept. 28, 2022), https://www.forrester.com/blogs/us-consumer-privacy-attitudes-in-2022/ (last accessed April 4, 2025).

and browsing history (84%).[47]

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

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

294. The template communications Google provides to school personnel include language intended to chill parental objections. For example, Google encourages school districts to describe "how not providing consent to use Google services will impact the educational experience."[48] Such language is coercive and exploitative.

295. Indeed, Google's Gemini agrees that this arrangement "can indeed place parents in a position where they feel they must choose between their child's right to privacy and their access to a full education."

296. Children and their parents are thus particularly vulnerable and disempowered to protect themselves against Google's policies and practices.

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

298. Google thus forces parents to choose between equal access to education on the one hand, and other basic rights belonging to themselves and their children, such as their rights to privacy and property on the other.

---

[47] *Polling Memo: Parents' Views on Children's Digital Privacy and Safety*, TRUSTED FUTURE (2022), https://trustedfuture.org/childrens-digital-privacy-and-safety/ (last accessed April 4, 2025).

[48] Google, *Google Workspace Admin Help: Notice Template for Schools When Gathering Parent or Guardian Consent*, https://support.google.com/a/answer/7391849?hl=en (last accessed April 4, 2025).

VI. Google's nonconsensual data practices are unfair and unlawful.

299. Google has generated enormous profits through collection and analysis of the Stolen Information—which it took from school-aged children without their or their parents' knowledge or consent, and without compensating them for the value of that information.

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

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

VII. Plaintiff-specific allegations.

A. Plaintiffs used Google's Products in the K-12 education setting, which collected and used Plaintiffs' data.

302. The minor Plaintiffs used Chromebooks, Chrome OS, the Chrome browser, and Workspace for Education in the course of their K-12 public education.

303. Those Products are owned, controlled, and operated by Google.

304. Google has shared and continues to share the Stolen Information across its suite of products.

305. Google processes and uses information generated, uploaded, or stored in Google databases, including the Stolen Information, for commercial purposes.

306. Google uses the Stolen Information to develop, improve, and market its products and other commercial purposes.

307. Google uses the Stolen Information to develop its analytics tools, which it sells to

Plaintiffs' schools and school districts.

308. Google has provided third parties the Stolen Information for commercial purposes, including identification, targeting, influence, and decision-making purposes.

B. Plaintiffs did not consent to Google's generation, collection, and use of their data.

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

310. Google never notified the Plaintiff parents that their minor children were using Google's Products.

311. Plaintiffs were never provided all material terms regarding Google's data policies and practices, such as what of their personal information that Google would collect, how it would be used, or who else would have access to it.

312. Plaintiff parents were unable to obtain adequate information relating to or arising from Google's generation, collection, or use of their children's data.

313. Plaintiffs did not consent to Google's data policies and practices. Any purported consent was not informed, was not provided by a person with proper authority, was not voluntary, and was not supported by sufficient consideration commensurate with the level of Google's surveillance and profiteering.

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

314. Plaintiffs requested access to the data Google generated about and collected from them through its Products that Plaintiff minor children were required to use.

315. Google responded by refusing to provide Plaintiffs such access.

316. Google instead directed Plaintiffs to contact their schools about obtaining access to their own information that Google generated about and collected about them.

317. Google has a policy of denying parents access to the data it collects about them and their children, and instead requires that parents request access to such data through their school administrators.

318. On information and belief, schools do not have access to or control over all the Stolen Information.

319. To the extent schools do have access to the Stolen Information, they are unable or unwilling to share all such information with students or their parents. Google facilitates this obstruction by providing administrators the ability to limit what Stolen Information students and parents have access to.

320. Google's policy of denying parents access to data constructively ensures that Plaintiffs and putative Class members have no way to access, review, or control their data.

321. Google may not absolve itself of its duty to provide parents access to their children's data by unilaterally shifting that duty to schools.

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

322. Google's data practices harmed Plaintiffs in a number of material ways. Because Google refuses to disclose information critical to facilitating a meaningful understanding of its data practices, discovery is necessary to fully understand and identify the nature and details of these harms.

323. Google's data policies and practices harmed Plaintiffs by invading their privacy.

324. Google's data policies and practices have compromised Plaintiffs relationships with various school personnel.

325. Google's data policies and practices harmed Plaintiffs by diminishing the value of their data.

326. Google's data policies and practices harmed Plaintiffs by denying them access to their own data.

327. Google's data policies and practices harmed Plaintiffs by denying them control over their own data, including whether it existed in the first place.

328. Google's data policies and practices harmed Plaintiffs by using their data to build intimate digital dossiers about them, and by using and disclosing those dossiers to untold third parties for unknown purposes.

329. Google's data policies and practices harmed Plaintiffs by subjecting them to unfair,

deceptive practices that have prevented them from understanding the full extent of how they may have been harmed by those practices.

330. Google's data policies and practices harmed Plaintiffs by failing to compensate them for their property or labor, which it has used to fuel its highly lucrative business.

CLASS ACTION ALLEGATIONS

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

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

> All persons in the United States who attend or attended a K-12 public school who used Google's Products, defined herein as the Chromebook, Chrome OS, Chrome browser, and Workspace for Education, as part of their schooling.

333. Plaintiffs A.G. and Z.G. seek to represent a state-only subclass of students ("California Subclass") under the law of the State of California defined as:

> All persons in California who attend or attended a K-12 public school who used Google's Products, defined herein as the Chromebook, Chrome OS, Chrome browser, and Workspace for Education, as part of their schooling.

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

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

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

337. Excluded from the Classes are: (1) the Court (including any Judge or Magistrate presiding over this action and any members of their chambers and families); (2) Google, its subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them

have a controlling interest and its officers, directors, employees, affiliates, or legal representatives; (3) persons who properly and timely request exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel, Classes' counsel, and Google's counsel; and (6) the legal representatives, successors, and assigns of any such excluded person.

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

339. **Numerosity**: Each member of the Classes likely consists of at least thousands of individuals. Accordingly, members of the Classes are so numerous that joinder of all members is impracticable. Class members may be identified from Google's records.

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

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

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

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

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

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

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

e. Whether Google failed to obtain informed and voluntary consent to collect data from Plaintiffs and Class members;

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

g. Whether Google's practice of intercepting, receiving, or collecting data from Plaintiffs and Class members violated state and/or federal privacy laws;

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

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

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

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

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

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

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

344. **California law applies to all Class members**: California's substantive laws apply to

every Plaintiff and member of the Class, regardless of where in the United States the Class member resides because Plaintiffs' and Class members' injuries emanate from Google's actions in California. Upon information and belief, each actionable decision related to the creation, implementation, maintenance, monetization, and concealment of the data-harvesting scheme in the United States was made from Google's California headquarters by its respective executives and employees located in California. Further, Google's own Terms of Service explicitly requires users to "agree that: (i) the Service shall be deemed solely based in California; and (ii) the Service shall be deemed a passive one that does not give rise to personal jurisdiction over Google, either specific or general, in jurisdictions other than California. The Agreement shall be governed by the internal substantive laws of the State of California, without respect to its conflict of laws principles." By choosing California law for the resolution of disputes covered by its Terms of Service, Google concedes that it is appropriate for this Court to apply California law to the instant dispute to all Class members. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class members under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the United States' Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by the Plaintiffs and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Google's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible. The application of California laws to Plaintiffs and the Classes is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Classes and California has the greatest interest in applying its laws here.

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

CAUSES OF ACTION

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

346. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth herein.

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

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

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

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

351. Google has been authorized by governmental entities to perform a function that is traditionally a public function performed by the government, namely, collecting and storing education records.

352. Google is jointly engaged with state officials in the prohibited action and, as such, is acting under color of law.

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

354. Google's data policies and practices violate the constitutional rights of Plaintiffs and Class members, including their Fourth Amendment right to be free from unreasonable searches and seizures.

355. Google's data policies and practices far exceed any legitimate authority to act on the government's behalf.

356. Google's surreptitious and persistent surveillance of the Plaintiffs' and Class members' activity as they use and interact with its products as described herein is a violation of their Fourth

Amendment rights.

357. Google's persistent, indiscriminate, and maximally intrusive surveillance data policies and practices are not justified by any legitimate governmental interest.

358. Google's nonconsensual taking of personal and private information of Plaintiffs and Class members for its own financial gain as described herein is a violation of their Fourth Amendment rights.

359. Google has admitted that the kinds of personal and private information it takes from children as described herein is "sensitive" and "would paint an incredibly intimate picture of an individual's life," and that the unlawful collection of such information poses "civil liberties and human rights concerns[.]"

360. No compelling state interest outweighs these rampant violations of Plaintiffs' and Class members' constitutional rights.

361. Google is therefore liable to Plaintiffs and Class members for their costs, including attorney fees and expert fees under 42 United States Code section 1988.

Count II: Violation of 42 U.S.C. § 1983 – Fourteenth Amendment

362. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth herein.

363. To state a claim under 42 United States Code section 1983, a plaintiff must allege that the defendant, acting under color of law, deprived the plaintiff of a federally protected right.

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

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

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

367. Google has been authorized by governmental entities to perform a function that is

traditionally a public function performed by the government, namely, collecting and storing education records.

368. Google is jointly engaged with state officials in the prohibited action and, as such, is acting under color of law.

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

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

371. Google's nonconsensual taking of personal and private information of Plaintiffs and Class members for its own financial gain as described herein is a violation of their Fourteenth Amendment rights.

372. The types of information that Google generates and extracts from Plaintiffs and Class members is information that is constitutionally protected.

373. Google has admitted that the personal and private information it takes from children as described herein is "sensitive" and "would paint an incredibly intimate picture of an individual's life," and that the unlawful collection of such information poses "civil liberties and human rights concerns[.]"

374. Plaintiffs and Class members have an interest in avoiding disclosure of personal matters.

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

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

377. The privacy interests at issue—and Google's infringement of those interests—are of constitutional importance.

378. Google has far exceeded whatever authority it has to act under the color of law on behalf of schools and school districts in the collection of the personal and private information of Plaintiffs and Class members.

379. Google does not employ adequate safeguards to prevent further unauthorized disclosure of Plaintiffs' and Class members' private information.

380. Google's data policies and practices expose children to significant risks, including the risk of identity theft.

381. Google's denial of and policy of denying Plaintiffs' and Class members' access to their own personal and private information violations their constitutional rights.

382. Google's denial of, and policy of denying, Plaintiffs' and Class members' ability to control their own personal and private information violates their constitutional rights.

383. These harms are exacerbated by the mandatory and surreptitious nature of Google's Products, and their use in a compulsory environment by children.

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

385. Google is therefore liable to Plaintiffs and Class members for their costs, including attorney fees and expert fees under 42 United States Code section 1988.

Count III: Violation of the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*

386. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth herein.

387. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

388. The Wiretap Act protects both the sending and receipt of communications.

389. 18 United States Code section 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

390. Google's actions in intercepting and tracking user communications were intentional. Upon information and belief, Google is aware that it is intercepting communications and has taken no remedial actions.

391. Google's interception of internet communications that the Plaintiffs and Class members were sending and receiving was done contemporaneously with the Plaintiffs' and Class members' sending and receipt of those communications.

392. The communications intercepted by Google included "contents" of electronic communications made from the Plaintiffs and Class members to websites and other web properties other than Defendant's in the form of detailed URL requests, webpage browsing histories, search queries, and other information that Plaintiffs and the Class members sent to those websites and for which Plaintiffs received communications in return from those websites.

393. These transmissions were tracked and intercepted without authorization and are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 United States Code section 2510(12).

394. The following constitute "devices" within the meaning of 18 United States Code section 2510(5):

a. The computer codes and programs that Google used to track the Plaintiffs' and Class members' communications;

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

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

d. Google's servers; and

e. The plan that Google carried out to effectuate its tracking and interception of the Plaintiffs' and Class members' communications.

395. Google, in its conduct alleged here, was not providing an "electronic communication service" as that term is defined in 18 United States Code section 2510(12) and is used elsewhere in

the Wiretap Act. Google was not acting as an Internet Service Provider (ISP).

396. Google was not an authorized party to the communications because the Plaintiffs and Class members were unaware of Google's interceptions and did not knowingly send any communications to Google when Google intercepted the communications between the Plaintiffs and web properties other than Google's. Google could not manufacture its own status as a party to the Plaintiffs' and Class members' communications with others by surreptitiously redirecting or intercepting those communications.

397. Plaintiffs and Class members did not consent to Google's continued gathering of their communications.

398. After intercepting the communications, Google then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 United States Code section 2511(1)(a).

399. As a result of this conduct, the Court may assess statutory damages to Plaintiffs and Class members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Google in the future, and reasonable attorneys' fees and other litigations costs reasonably incurred.

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

400. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth herein.

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

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

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

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

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

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

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

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

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

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

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

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

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

d. Google's servers;

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

f. The plan Google carried out to effectuate its tracking and interception of the Plaintiffs' and Class members' communications.

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

409. Google aided and abetted numerous third parties in unlawfully intercepting protected communications belonging to Plaintiffs and Class members.

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

411. Pursuant to California Penal Code section 637.2, Plaintiffs and Class members have been injured by the violations of California Penal Code sections 631 and 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

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

412. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth herein.

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

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

415. Google effectively charged Plaintiffs and Class members and was enriched by

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

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

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

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

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

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

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

421. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth

herein.

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

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

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

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

426. To establish liability under the "unfair" prong, Plaintiffs and Class members need not establish that these statutes were actually violated, although the allegations herein establish that they were. The foregoing allegations are tethered to underlying constitutional, statutory or regulatory provisions; describe practices that are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers; and show that negative impact of Google's practices on school-aged children and their parents far outweighs the reasons, justifications, and motives of Google.

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

428. The foregoing allegations also establish liability under the "fraudulent" prong, as Google's false and misleading representations and omissions 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.

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

value of their private and personally identifiable data and content.

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

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

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

432. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth herein.

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

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

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

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

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

a. ECPA;

b. COPPA;

c. CIPA;

d. CDAFA;

e. The Fourth Amendment right to privacy contained on school-issued and/or personal computing devices, including all of their activity on their devices;

f. The Fourteenth Amendment right to informational privacy; and

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

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

439. Google's actions constituted a serious invasion of privacy in that it:

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

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

c. Violated laws, including the ECPA, COPPA, CIPA, and CDAFA;

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

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

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

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

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

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

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

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

Count VIII: Intrusion Upon Seclusion

444. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth herein.

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

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

447. Google's tracking and interception were not authorized by the Plaintiffs and Class members.

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

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

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

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

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

453. Google understands and admits the sensitivity of the information it generates and collects and acknowledges that such information implicates fundamental human rights.

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

Count IX: Unjust Enrichment

455. Plaintiffs incorporate by reference paragraphs 1 through 345 as though fully set forth herein.

456. Google has unjustly received benefits at the expense of Plaintiffs and Class members.

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

458. Google has derived profits and other tangible benefits from its collection of Stolen Information, without which Google could not as effectively have grown its business, acquired numerous other tangible and intangible assets, developed other products, supported myriad data-sharing agreements, and, as of the date of this filing, stand at a more than $1.8 trillion valuation.

Google has also directly and substantially profited from its use, storage, aggregation, and sale of Plaintiffs' and Class members' data. Indeed, Plaintiffs' and Class members' data is the fuel that powers Google's ever-growing suite of "personalized" products and services marketed for use by children in K-12 education.

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

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

461. Google did not and made no efforts to determine whether Plaintiffs' and Class Members' use of its Products in compulsory K-12 environments was voluntary.

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

463. Google harmed Plaintiffs and Class members by, among other harms, subjecting them to commercial manipulation and continuous surveillance; abridging parents' right to parent as they choose; invading their privacy; denying their due process rights by subjecting them to opaque, unreviewable data practices; forcing them to choose between their right to an education and other fundamental rights; and failing to compensate them for their property and labor.

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

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

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

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

RELIEF REQUESTED

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

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

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

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

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

e. Costs to the extent provided by law; and

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

JURY TRIAL DEMAND

Plaintiffs demand a jury trial for all claims so triable.

Dated: April 7, 2025

Respectfully submitted,

By: */s/ Rebecca A Peterson*

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

Daniel E. Gustafson (*pro hac vice* forthcoming)
dgustafson@gustafsongluek.com
Catherine Sung-Yun Smith (*pro hac vice forthcoming)*
csmith@gustafsongluek.com
Shashi K. Gowda (*pro hac vice* forthcoming)
sgowda@gustafsongluek.com
GUSTAFSON GLUEK, PLLC
Canadian Pacific Plaza
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
Tel.: (612) 333-8844
Fax: (612) 339-6622

Rebecca A. Peterson (241858)
RPeterson@4-justice.com
GEORGE FELDMAN MCDONALD, PLLC
1650 West 82nd Street, Suite 880
Bloomington, MN 55431
Tel.: (612) 778-9595
Fax: (888) 421-4173

David George (*pro hac vice* forthcoming)
DGeorge@4-Justice.com
Brittany Sackrin (*pro hac vice* forthcoming)
GEORGE FELDMAN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Tel.: (561) 232-6002
Fax: (888) 421-4173

Lori G. Feldman (*pro hac vice* forthcoming)
LFeldman@4-justice.com
Michael Liskow (SBN 243899)

MLiskow@4-Justice.com
GEORGE FELDMAN MCDONALD, PLLC
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel.: (917) 983-9321
Fax: (888) 421-4173

Counsel for Plaintiffs and the Proposed Class

CIVIL COVER SHEET

This civil cover sheet does not replace or supplement the filing and service of pleadings or other papers. The information on this form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket. Instructions are on the reverse of this form.

I. PLAINTIFF(S)

JOEL SCHWARZ, on behalf of his minor child B.S., EMILY DUNBAR, on behalf of her minor child H.D., and MICHAEL GRIDLEY and ELIZABETH GRIDLEY, on behalf of their minor children A.G. and Z.G., individually and on behalf of all others similarly situated,

County of Residence of First Listed Plaintiff: Montgomery County, Maryland
Leave blank in cases where United States is plaintiff.

Attorney or Pro Se Litigant Information *(Firm Name, Address, and Telephone Number)*

George Feldman McDonald, PLLC; Rebecca A. Peterson
1650 W. 82nd Street, Suite 880, Bloomington, Minnesota 55431

DEFENDANT(S)

Google, LLC

County of Residence of First Listed Defendant:
Use ONLY in cases where United States is plaintiff.

Defendant's Attorney's Name and Contact Information *(if known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ U.S. Government Plaintiff
- ☐ Federal Question *(U.S. Government Not a Party)*
- ☐ U.S. Government Defendant
- ☒ Diversity

III. CAUSE OF ACTION

Cite the U.S. Statute under which you are filing: *(Use jurisdictional statutes only for diversity)*
28 U.S.C.§ 1332(d)

Brief description of case: Violations of Plaintiffs' and Class Members' privacy rights.

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☒ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 U.S.C. § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ Original Proceeding
- ☐ Removed from State Court
- ☐ Remanded from Appellate Court
- ☐ Reinstated or Reopened
- ☐ Transferred from Another District
- ☐ Multidistrict Litigation–Transfer
- ☐ Multidistrict Litigation–Direct File

VI. FOR DIVERSITY CASES ONLY: CITIZENSHIP OF PRINCIPAL PARTIES

(Place an "X" in One Box for Plaintiff and One Box for Defendant)

Plaintiff	Defendant	
☐	☒	Citizen of California
☒	☐	Citizen of Another State
☐	☐	Citizen or Subject of a Foreign Country
☐	☐	Incorporated or Principal Place of Business In California
☐	☐	Incorporated and Principal Place of Business In Another State
☐	☐	Foreign Nation

VII. REQUESTED IN COMPLAINT

- ☑ Check if the complaint contains a **jury demand.**
- ☐ Check if the complaint contains a **monetary demand**. Amount:
- ☑ Check if the complaint seeks **class action** status under Fed. R. Civ. P. 23.
- ☐ Check if the complaint seeks a **nationwide injunction** or Administrative Procedure Act vacatur.

VIII. RELATED CASE(S) OR MDL CASE

Provide case name(s), number(s), and presiding judge(s).

IX. DIVISIONAL ASSIGNMENT pursuant to Civil Local Rule 3-2

(Place an "X" in One Box Only) ☒ SAN FRANCISCO/OAKLAND ☐ SAN JOSE ☐ EUREKA-MCKINLEYVILLE

DATE 04/07/2025 **SIGNATURE OF ATTORNEY OR PRO SE LITIGANT** /s/ Rebecca A. Peterson

COMPLETING THE CIVIL COVER SHEET

Complete the form as follows:

I. Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.

Attorney/Pro Se Litigant Information. Enter the firm name, address, telephone number, and email for attorney of record or pro se litigant. If there are several individuals, list them on an attachment.

II. Jurisdiction. Under Federal Rule of Civil Procedure 8(a), pleadings must establish the basis of jurisdiction. If multiple bases for jurisdiction apply, prioritize them in the order listed:

(1) *United States plaintiff*. Jurisdiction based on 28 U.S.C. §§ 1345 and 1348 for suits filed by the United States, its agencies or officers.

(2) *United States defendant.* Applies when the United States, its agencies, or officers are defendants.

(3) *Federal question*. Select this option when jurisdiction is based on 28 U.S.C. § 1331 for cases involving the U.S. Constitution, its amendments, federal laws, or treaties (but use choices 1 or 2 if the United States is a party).

(4) *Diversity of citizenship.* Select this option when jurisdiction is based on 28 U.S.C. § 1332 for cases between citizens of different states and complete Section VI to specify the parties' citizenship. Note: Federal question jurisdiction takes precedence over diversity jurisdiction.

III. Cause of Action. Enter the statute directly related to the cause of action and give a brief description of the cause. Do not cite jurisdictional statutes unless jurisdiction is based on diversity. Example: U.S. Civil Statute: 47 U.S.C. § 553. Brief Description: Unauthorized reception of cable service.

IV. Nature of Suit. Check one of the boxes. If the case fits more than one nature of suit, select the most definitive or predominant.

V. Origin. Check one of the boxes:

(1) *Original Proceedings*. Cases originating in the United States district courts.

(2) *Removed from State Court*. Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C. § 1441. When the petition for removal is granted, check this box.

(3) *Remanded from Appellate Court*. Check this box for cases remanded to the district court for further action, using the date of remand as the filing date.

(4) *Reinstated or Reopened*. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) *Transferred from Another District*. Check this box for cases transferred under Title 28 U.S.C. § 1404(a). Do not use this for within-district transfers or multidistrict litigation (MDL) transfers.

(6) *Multidistrict Litigation Transfer*. Check this box when a multidistrict (MDL) case is transferred into the district under authority of Title 28 U.S.C. § 1407.

(7) *Multidistrict Litigation Direct File.* Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

VI. Residence (citizenship) of Principal Parties. Mark for each principal party *only* if jurisdiction is based on diversity of citizenship.

VII. Requested in Complaint.

(1) *Jury demand.* Check this box if plaintiff's complaint demanded a jury trial.

(2) *Monetary demand*. For cases demanding monetary relief, check this box and enter the actual dollar amount being demanded.

(3) *Class action.* Check this box if plaintiff is filing a class action under Federal Rule of Civil Procedure 23.

(4) *Nationwide injunction.* Check this box if plaintiff is seeking a nationwide injunction or nationwide vacatur pursuant to the Administrative Procedures Act.

VIII. Related Cases. If there are related pending case(s), provide the case name(s) and number(s) and the name(s) of the presiding judge(s). If a short-form MDL complaint is being filed, furnish the MDL case name and number.

IX. Divisional Assignment. Identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated." Note that case assignment is made without regard for division in the following case types: Property Rights (Patent, Trademark and Copyright), Prisoner Petitions, Securities Class Actions, Anti-Trust, Bankruptcy, Social Security, and Tax.