Victor J. Sandoval (SBN 344461)
ALMEIDA LAW GROUP LLC
3415 S. Sepulveda Blvd., Suite 1121
Los Angeles, California 90034
Telephone: (562) 534-5907
victor@almeidalawgroup.com

Counsel for Plaintiff & the Putative Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

EDWARD LOMINCHAR, *on behalf of himself and all others similarly situated,* Plaintiff, vs. **TIKTOK USDS JOINT VENTURE, LLC,** Defendant.	**Case No.** 2:26-cv-9700 **CLASS ACTION COMPLAINT** **1. VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2511, *ET SEQ.*** **2. VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE § 631** **3. VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE § 632** **4. INTRUSION UPON SECLUSION** **5. INVASION OF PRIVACY** **6. UNJUST ENRICHMENT** **DEMAND FOR JURY TRIAL**

Plaintiff Edward Lominchar, individually and on behalf of all others similarly situated, brings this class action lawsuit against Defendant TikTok USDS Joint Venture, LLC, d/b/a Gauth AI ("Gauth" or "Defendant"), and alleges the following based upon personal knowledge as to himself and his actions, knowledge, and experiences, and upon information and good faith belief as to all other matters.

INTRODUCTION

1. This class action lawsuit challenges Defendant's practice of secretly transmitting the private communications, educational queries, and personal data of the users of its artificial-intelligence homework-help service, Gauth (accessible at Gauth.ai and Gauthmath.com) (the "Platform"), to Google LLC ("Google") without the knowledge or consent of its users.

2. Defendant operates the Platform as a consumer-facing artificial intelligence service that purports to assist students with solving homework problems as well as helping them with other educational questions.

3. Users—many of whom are children and adolescents—type or photograph their schoolwork into the Platform and receive AI-generated explanations and answers in response.

4. The Platform's users are students. In using the Platform, these users provide deeply sensitive educational information, including the full text of homework questions and academic problems they are unable to solve on their own; the courses and subjects they are studying; the academic level at which they are working; the schools and assignments they are completing; personal essays and writing prompts (which frequently disclose information about the student's family, mental health, identity, and life circumstances); and detailed records of their academic struggles, weaknesses, and educational progress (collectively, the "Sensitive Educational Information").

5. A substantial portion of the Platform's user base consists of minors.

6. Defendant markets the Platform to students of all ages including, but not limited to, primary, middle, and high school students, and the Platform is freely accessible to minors at Gauth.ai and Gauthmath.com without payment, registration, or any age verification.

7. State legislatures, federal agencies, professional trade groups, and industry practitioners alike have recognized the heightened privacy interests surrounding educational data in general and children's educational data specifically.[1]

8. Users of the Platform reasonably expect that the Sensitive Educational Information that they provide to Defendant—especially the text of academic questions submitted for AI assistance—will remain private and confidential, visible only to Defendant for the purpose of generating an answer.

9. Nothing Defendant presents to its users disturbs or alters that expectation.

10. Defendant does not require users to encounter any privacy disclosure before using the Platform.

11. Rather, in the normal use of the Platform, a user will load the Platform, submit an academic question, and receive an AI-generated answer without ever

[1] *See, e.g., State Student Privacy Laws*, Public Interest Privacy Center, https://publicinterestprivacy.org/resources/state-student-privacy/ (last visited August 27, 2026) (noting that since 2014, more than one thousand student privacy bills have been introduced in all 50 states and that state policymakers have passed nearly 150 student privacy laws in 47 states and the District of Columbia); *Student Privacy Pledge*, Future of Privacy Forum, https://fpf.org/student-privacy-pledge/ (last visited August 27, 2026) (describing the legally enforceable industry pledge created by the Future of Privacy Forum and the Software & Information Industry Association, signed by nearly 500 ed tech companies, committing signatories not to sell student personal information or use it for non-educational purposes).

being shown—or being required to open, scroll through, or accept—any privacy policy, notice, or consent screen.[2]

12. At no point does Defendant notify users that it transmits the full text of their precise questions or the academic content they submit to Google for advertising, analytics, and profiling purposes.

13. Users are therefore given no opportunity to learn of, much less to consent to, the interception before it occurs.

14. Unbeknownst to users, Defendant has embedded the Google Analytics tracking technology ("Google Analytics") within the Platform.

15. That tracking code secretly intercepts and transmits to Google, in real time: (a) the full text of the academic question or content the user has submitted to the Platform for AI assistance; (b) a persistent identifier, the Google Analytics "cid", that Google uses to identify the user across sessions, devices, and properties, and that, on information and belief, Google links to the user's Google account, Google Workspace for Education identity, or other Google-identifiable profile; and (c) granular engagement data, including the timing, duration, and depth of the user's interactions with the Platform.

16. These transmissions occur without any notice to the user and without the user's consent. They occur every time a user submits an academic question to the Platform and on every page or screen on which Google Analytics is deployed.

17. These transmissions, when aggregated, disclose an extraordinarily sensitive portrait of each user, including:

a. The specific subjects and courses the user is studying;

[2] *Gauth Privacy Policy*, https://www.gauthmath.com/policy (last visited August 27, 2026).

b. The user's academic level, grade, and educational ability;

c. The user's specific academic difficulties and the topics with which the user struggles;

d. Personal information embedded in the questions themselves (including, in many cases, students' names, schools, teachers, and the content of assignments concerning the student's family life, mental health, and personal circumstances);

e. The frequency and intensity of the user's reliance on the Platform; and

f. The user's inferred academic ability, drawn from the difficulty of the material the user cannot complete unaided.

18. Google then combines this information with the comprehensive profiles it already maintains about each user from its own services (including Search, Gmail, YouTube, Chrome, Android, and Google Workspace for Education) and from the millions of other applications and websites in which Google Analytics is embedded, to build, refine, and monetize cross-platform behavioral profiles that are then offered to third-party advertisers.

19. The nonconsensual disclosure or mishandling of this data can cause concrete and irreversible harm.

20. Educational data and academic queries are among the most sensitive categories of personal information that exist for a young person.

21. Disclosure can impose serious downstream consequences on unsuspecting students, including:

a. Surveillance by school administrators;

b. Narrowing of educational and commercial opportunities when transmitted data identifies the subjects in which a student is failing and how often the student cannot complete work unaided;

c. Subjection of students by Google and its advertising customers to advertising based on perceived inferred ability tiers, educational challenges, and learning disabilities;

d. Transmission of unwanted advertisements, or withholding of desired notice of, available tutoring services, test-preparation programs, scholarships, and vocational offerings, which a student may or may not be shown based on inferences the student cannot see, review, or correct;

e. Exposure to age-inappropriate advertising and predatory data brokers that follow the student across schools and into adulthood as a permanent digital record of their academic struggles; and

f. Disclosure of deeply private aspects of the student's life.

22. Because educational data touches on the developmental autonomy and future opportunities of a child, Defendant's obligation to safeguard it was correspondingly grave.

23. Defendant's secret transmission of users' private communications and Sensitive Educational Information to Google violates the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511, 2520 ("ECPA"); the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* ("CIPA"); and constitutes intrusion upon seclusion, invasion of privacy, and unjust enrichment.

PARTIES

24. Plaintiff Edward Lominchar is a natural person who, at all times relevant hereto, has resided (and continues to reside) in Miami, Florida. Plaintiff was seventeen years old and enrolled as a high school student when he first used the Platform and remained a minor throughout the period in which he used the Platform from approximately December 2024 through at least January 2026 to obtain assistance with his academic coursework; Plaintiff has since reached the age of majority.

25. Defendant TikTok USDS Joint Venture, LLC is a Delaware limited liability company with its principal place of business in Culver City, California. Defendant owns and operates the Platform, the websites at Gauth.ai and Gauthmath.com, through which it transacts business with users residing throughout the United States, including in California.

26. Defendant directs the Platform at users throughout the United States, including a substantial number of minor users, and integrates the Platform with Google's analytics and advertising ecosystem to transmit users' Sensitive Educational Information to Google for Google's own commercial use.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because (a) this is a class action lawsuit in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; (b) there are more than 100 members of the proposed class; and (c) at least one member of the proposed class is a citizen of a State different from Defendant.

28. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises in part under the laws of the United States, specifically the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511, 2520.

29. The Court has supplemental jurisdiction over the state-law claims pursuant to 28 U.S.C. § 1367.

30. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, has purposefully availed itself of the privilege of conducting business in California by operating the Platform as a nationwide service accessible to California residents, and by directing its business activities toward users nationwide, including Plaintiff.

31. Defendant's tortious conduct, including its embedding of the Google Analytics tracking technology within the Platform to intercept the communications of users nationwide, took place via Defendant's servers in California.

32. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides in this District, and pursuant to 28 U.S.C. §

1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District, including Defendant's design and operation of the Platform, its embedding of the Google Analytics tracking technology, and the interception and transmission of users' Sensitive Educational Information directed from Defendant's principal place of business in this District.

FACTUAL ALLEGATIONS

I. DEFENDANT'S PLATFORM AND ITS USERS.

33. Defendant markets and operates the Platform as a free, AI-powered homework-help and tutoring service.[3]

34. Through the Platform, users—a substantial portion of whom are children and adolescents in primary, middle, high school, or college—type academic questions and receive AI-generated answers, explanations, and step-by-step solutions in response.[4]

35. Defendant markets the Platform under the Gauth and Gauthmath brand names and holds it out as a study companion for students.

36. The Platform is provided at no cost to users; Defendant monetizes the Platform through subscriptions, advertising relationships, and data-sharing relationships that Defendant does not disclose to its users.

37. To use the Platform's core functionality, a user submits an academic question to the Platform—by typing the question into a text field, uploading a

[3] *About Us*, https://www.gauth.com/aboutus, (last visited August 27, 2026).

[4] https://www.Gauth.com/aboutus (last visited August 27, 2026); *Gauth*, Google Play Store, https://play.google.com/store/apps/details?id=com.education.android.h.intelligence&hl=en_US (last visited August 27, 2026).

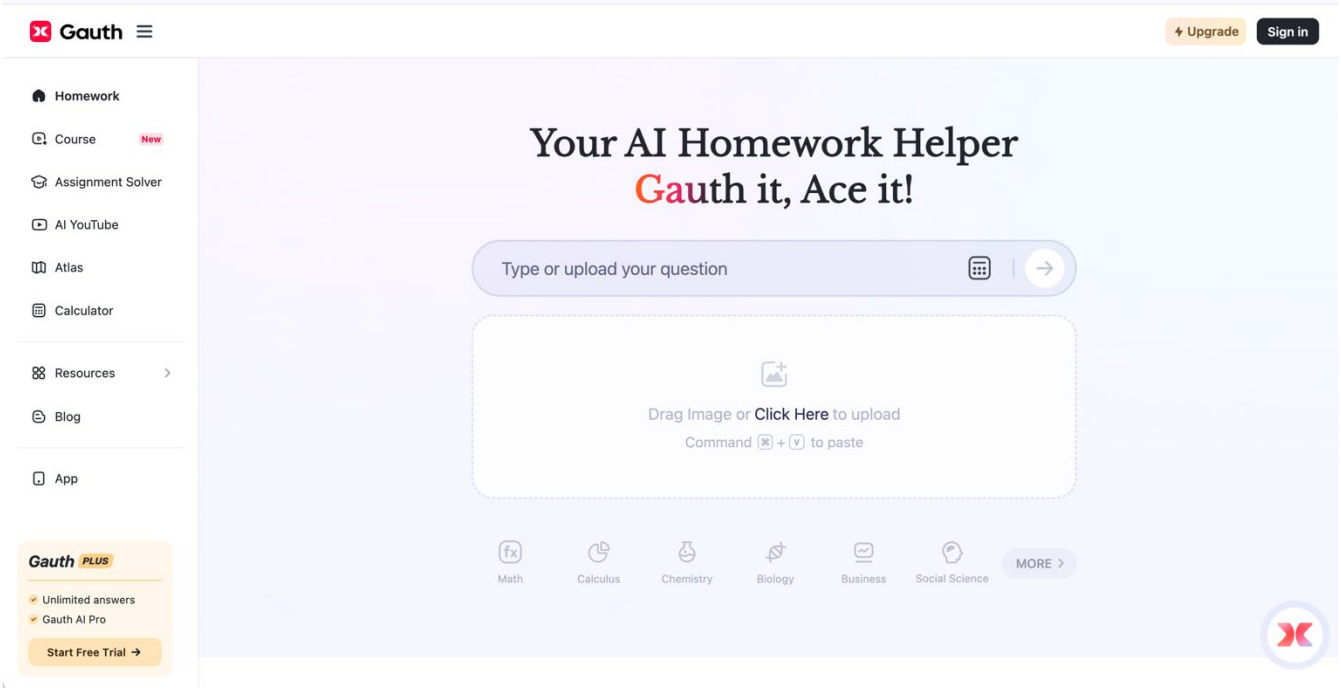
photograph or image of the question, or selecting a problem from the Platform's library—and the Platform returns an AI-generated response.

38. The full text of the question the user submits is the core communication between the user and Defendant; it is the input that the user reasonably expects Defendant to process, in private, for the sole purpose of generating an answer.

39. Defendant has designed the Platform to induce users to begin submitting academic questions immediately, before creating an account and before encountering any privacy disclosure.

40. A user who navigates to Gauth.ai or Gauthmath.com is presented with a text-entry field and a prompt inviting the user to type a question or upload a photograph of a problem, and upon submission the Platform returns an AI-generated response.

41. No registration, sign-in, or account is required to use that functionality.



42. At no point in that flow is the user required to review, scroll past, click through, or affirmatively assent to Defendant's Privacy Policy.

43. Defendant presents no interstitial, modal, banner, checkbox, or other disclosure conveying the Privacy Policy—or any description of Defendant's data-sharing practices—to the user before the user's first use of the Platform.

44. The Privacy Policy is instead available only through a hyperlink that the user must independently locate and affirmatively click, and that the Platform never requires the user to open.

45. By design, therefore, the Google Analytics tracking code described below begins intercepting and transmitting user data—including the full text of the user's first academic question—from the moment the user loads the Platform and submits that question.

46. That interception and transmission occurs before the user has created an account, before the user has been presented with any privacy disclosure, and before the user has had any opportunity to review the Privacy Policy or to give or withhold consent.

47. Defendant prompts users to register for an account only after they have already used the Platform and submitted academic questions to it.

48. Account registration therefore occurs, if at all, only after Defendant has already intercepted the user's Sensitive Educational Information and transmitted it to Google.

49. Defendant also collects from many of its users personally identifying information including the user's name, email address, age or grade level, and account credentials, as well as device identifiers and other technical data.

50. For users who sign in using a Google account—including a Google Workspace for Education account provided by the user's school—Defendant additionally has access to Google-issued identifiers that link the user's Platform activity to a Google-identifiable identity.

51. The content of a user's engagement with the Platform—including the specific homework questions the user is unable to solve, the subjects in which the user is struggling, the personal information the user includes in their questions (such as essay drafts, journal entries, or biographical context), the frequency with which the user seeks help, and the time of day at which the user uses the Platform—is the kind of information that a reasonable user would expect to remain confidential between the user and Defendant.

52. Educational data and academic queries are widely recognized to be among the most sensitive categories of personal information, particularly when associated with minors.[5]

53. The specific subjects a student is studying, the questions a student cannot answer without assistance, the personal essays and writing prompts a student completes, the content of a student's assignments, and the patterns and intensity of a student's reliance on outside help, each carry significant educational, reputational, and developmental implications, and each can cause substantial harm if disclosed to a school administrator, an advertiser, a data broker, or any unrelated third party.

54. State law across the country helps to frame the sensitivity of the information at issue here.

55. Florida's Protection of Children in Online Spaces Act, for example, limits how children's personal information can be processed, and restricts the profiling of a child by online entities. Fla. Stat. § 501.1735(2)(a)-(b).

[5] *See, e.g., Student Privacy Primer*, Student Privacy Compass (Future of Privacy Forum) (Oct. 2021), https://studentprivacycompass.org/resource/student-privacy-primer/ (last visited August 27, 2026); *The Policymaker's Guide to Student Data Privacy*, Public Interest Privacy Center, https://publicinterestprivacy.org/policymakers-guide-to-student-privacy/ (last visited August 27, 2026).

56. The persistent Google Analytics client identifier transmitted from the Platform is precisely such a unique identifier, and the cross-property behavioral profiling described above is precisely the profiling those provisions restrict. No part of that profiling is necessary to return an answer to a homework question.

57. In addition to Florida, a substantial and growing body of state law treats the personal information of minors as categorically sensitive and restricts the profiling of minors and the exploitation of their data for targeted advertising:

a. Colorado prohibits the collection or use of the personal data of consumers under eighteen for targeted advertising, profiling, or sale absent consent, and requires data-protection assessments for online services likely to be accessed by minors. Colo. Rev. Stat. § 6-1-1308.5.

b. Maryland prohibits the sale of personal data, and the processing of personal data for targeted advertising, where the controller knows or has reason to know that the consumer is under eighteen. Md. Code Ann., Com. Law § 14-4607.

c. Connecticut bars controllers from selling a minor's personal data or processing it for targeted advertising or profiling except in compliance with heightened consent requirements. Conn. Gen. Stat. §§ 42-515, et seq.

d. New York bars operators from processing a minor's personal data except with informed consent or where the processing is strictly necessary for an enumerated permissible purpose, such as delivering the product the minor actually requested. N.Y. Gen. Bus. Law §§ 899-ff, et seq.

e. California treats the personal information of a consumer known to be under sixteen as sensitive personal information and requires affirmative opt-in consent before that information may be sold or shared. Cal. Civ. Code § 1798.120(c).

f. Texas limits the collection of, and prohibits targeted advertising based on, the personal identifying information of known minors. Tex. Bus. & Com. Code §§ 509.001, et seq.

58. These statutes differ in their thresholds and mechanics, but they converge on the same issue, namely, that a minor's personal information may only be used to deliver the service the minor requested and may not be diverted into commercial profiling the minor never sought.[6]

59. Defendant's transmission of the full text of a minor's homework questions, bound to a persistent identifier, into Google's cross-property advertising ecosystem is the paradigm case of the conduct these legislatures acted to prevent.

60. Other state legislatures have specifically singled out student data for protection. *See* Illinois' Student Online Personal Protection Act, 105 ILCS 85/1, *et seq*.; New York Education Law § 2-d; California's Student Online Personal Information Protection Act, Cal. Bus. & Prof. Code §§ 22584, *et seq*.; *and* Colorado's Student Data Transparency and Security Act, Colo. Rev. Stat. §§ 22-16-101, *et seq*., each prohibit operators of online educational services from using student information for targeted advertising, from selling it, and from assembling non-educational profiles of students.

61. Those statutes show considered legislative judgment about the character of the information at issue: the questions a student cannot answer, the subjects in which the student struggles, and the pattern and intensity of the student's reliance on outside assistance are not ordinary commercial data, and their diversion to an advertising platform is the specific harm those legislatures acted to prevent.

---

[6] *See Little Users, Big Rules: Tracking Children's Privacy Legislation*, Mayer Brown (Jan. 2026), https://www.mayerbrown.com/en/insights/publications/2026/01/little-users-big-rules-tracking-childrens-privacy-legislation (last visited August 27, 2026); *Analyzing the 2025 Children's Privacy Laws and Regulations*, Troutman Pepper Locke Privacy + Cyber + AI Blog (Sept. 2025), https://www.troutmanprivacy.com/2025/09/analyzing-the-2025-childrens-privacy-laws-and-regulations/ (last visited August 27, 2026).

62. Federal agencies have also recognized that online educational and academic-assistance services collect data whose unauthorized use or sharing can cause material harm.

63. The Federal Trade Commission has warned that providers of education technology may not condition children's access to educational services on submission to commercial surveillance, and that student information collected to deliver an educational service may not be repurposed for unrelated commercial ends.

64. Those risks are especially acute for children and adolescents, including the risk of profiling, behavioral advertising directed at minors, and the permanent commercialization of records of a child's academic struggles.[7]

II. DEFENDANT'S SECRET USE OF THE GOOGLE TRACKING TECHNOLOGY.

65. Unbeknownst to its users, Defendant has embedded within the Platform Google Analytics tracking code that intercepts, copies, and transmits to Google the contents of users' private communications with Defendant—including, most significantly, the full text of the academic questions users submit to the Platform's AI for assistance.

[Remainder of page intentionally left blank]

[7] *See* Fed. Trade Comm'n, Press Release, *FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts* (May 22, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising; Fed. Trade Comm'n, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services* (Sept. 2024), https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services .

Question

Who was the Union general at Gettysburg

Gauth AI Solution

Answer

The Union general in command at the Battle of Gettysburg was **Major General George G. Meade**. He took command of the Army of the Potomac just days before the battle, replacing Major General Joseph Hooker. Meade successfully led the Union forces to a pivotal victory against Confederate General Robert E. Lee's Army of Northern Virginia.

Helpful Not Helpful

Headers Payload Preview Response Initiator Timing Cookies

ae	a
are	1
cid	1711223054.1778103961
frm	0
pscdl	noapi
rcb	18
sr	1920x1080
uaa	arm
uab	64
uafvl	Google%20Chrome;147.0.7727.102|Not.A%2FBrand;8.0.0.0|Chromium;147.0.7727.102
uam	
uamb	0
uap	macOS
uapv	15.4.0
uaw	0
ul	en-us
gaf	2
_s	1
tag_exp	0~115616986~115938465~115938469~118289195~118463261~118719171
sid	1778111186
sct	2
seg	1
dl	https://www.gauthmath.com/search-question?search=Who%20was%20the%20Union%20general%2 on=search&questionID=1986934286415494
dr	https://www.gauthmath.com/
dt	Who was the Union general at Gettysburg - Gauth

66. Google Analytics operates silently, in the background, without any visible indication to the user, and without any mechanism by which the user can consent to or opt out of it before it begins transmitting data.

III. HOW GOOGLE ANALYTICS OPERATES.

67. Google Analytics is a web-analytics service operated by Google LLC that enables website operators to collect granular data about user interactions with their sites, including page views, clicks, scrolls, form submissions, and custom events.

68. Google Analytics is typically deployed via a snippet of JavaScript embedded in the site's pages, often in conjunction with Google Tag Manager, which allows operators to deploy multiple tracking tags from a single container.[8]

69. By default, Google Analytics assigns each user a persistent unique client identifier ("cid"), which Google stores in a first-party cookie on the website domain.

70. This client identifier enables Google to link every page view, event, and interaction that a user performs on a given property to a single persistent identity, and—when combined with Google's own account ecosystem and the millions of other properties that deploy Google Analytics—to identify the user across sessions, devices, and properties.[9]

71. When Google Analytics is deployed on a website, each page view or event triggers a network request from the user's device to Google's collection

[8] *See Help Center*, https://support.google.com/analytics (last visited August 27, 2026).

[9] *See [GA4] Data collection, Google Analytics Help*, https://support.google.com/analytics/answer/11593727 (last visited August 27, 2026) (Google Analytics stores a client ID in a first-party cookie used to distinguish unique users and their sessions on the property).

endpoints at *.google-analytics.com, *.analytics.google.com, and related Google-operated domains.

72. That request carries, among other data: (a) the Google Tag ID of the property ("tid"); (b) the persistent client identifier ("cid"); (c) the full URL of the page the user is viewing ("dl"); (d) the full title of the page ("dt"); (e) the screen resolution and viewport of the device; (f) the language and timezone; (g) the event name ("en") being transmitted (for example, "page_view," "scroll," "click," "search," or operator-defined events); and (h) event parameters describing the event in detail. These parameters are configurable by the operator and are routinely used, as Defendant uses them, to capture the full text of user-submitted content and other granular behavioral signals.[10]

73. Once data is received at Google's collection endpoints, Google does not simply store that data for the operator's internal analytics.

74. Rather, Google uses that data (a) to power its Google Ads and Google Marketing Platform advertising products, including for audience building, retargeting, and cross-property profiling; (b) to improve its own machine-learning models; and (c) to associate the user's activity on the operator's property with the user's identity on Google's own services, including Search, YouTube, Gmail, Maps, Chrome, the Android operating system, and Google Workspace for Education.[11]

[10] *See* [GA4] Measurement Protocol Reference, Google Analytics Developer Guide, https://developers.google.com/analytics/devguides/collection/protocol/ga4 (last visited August 27, 2026).

[11] See Google Marketing Platform, https://marketingplatform.google.com/about/ (last visited August 27, 2026); Connect Google Ads to Google Analytics, Google Analytics Help, https://support.google.com/analytics/answer/9379420 (last visited August 27, 2026).

IV. DEFENDANT'S CONFIGURATION OF GOOGLE ANALYTICS ON THE PLATFORM.

75. Defendant has deployed Google Analytics (Google Analytics 4, or "GA4") on the Platform and has configured it to transmit to Google, in real time, the full text of the academic questions and other Sensitive Educational Information that users submit to the Platform's AI for assistance. Network traffic captured from a user's interaction with the Platform confirms that, when a user submits a question to the Platform, the user's device transmits to Google's servers, among other fields:

a. a Google Tag ID ("tid") identifying Defendant's Google Analytics property;

b. a persistent Google Analytics client identifier ("cid") that uniquely identifies the user across sessions and across the Platform, and that, on information and belief, Google associates with the user's Google account, Google Workspace for Education identity, or other Google-identifiable profile;

c. the document location ("dl") corresponding to the specific Platform URL on which the question was submitted;

d. an event name ("en") and event parameters that contain the full text of the academic question or other content the user submitted to the Platform, including, where applicable, the text of math problems, science problems, reading-comprehension passages, essay prompts, and personal-writing prompts;

e. session identifiers, session counts, and engagement flags that disclose the frequency, duration, and depth of the user's reliance on the Platform; and

f. device characteristics, including screen resolution, language, operating-system version, and a user agent identifying the browser and device used to access the Platform.

76. These transmissions occur in real time and without any intervening notice to the user. At the moment a user submits a question to the Platform, Defendant's embedded Google Analytics code simultaneously transmits the contents of that question (the precise text the user has typed, photographed, or otherwise entered) to Google, together with a persistent identifier linking that submission to the user's device.

77. Because users of the Platform are disproportionately students—many of whom are minors—the content of the transmitted questions routinely discloses information of extraordinary sensitivity, including (i) personally identifiable details about the user (such as the student's name, school, or teacher when these are embedded in a homework prompt or essay draft); (ii) details about the user's family life, mental health, or personal circumstances (which frequently appear in personal-essay assignments and college-application drafts); (iii) details about the user's academic difficulties and the subjects in which the user struggles; and (iv) patterns of assistance-seeking that the user reasonably believed to be private and confidential.[12]

78. Google uses the data it receives from the Platform for its own independent commercial purposes, including to associate the user's educational activity with the user's identity on Google's own services (including Search, Gmail, YouTube, Chrome, Android, and, for students, Google Workspace for Education), to power Google's advertising products, and to refine the user's behavioral profile

[12] *See, e.g.*, U.S. Dep't of Educ., Protecting *Student Privacy While Using Online Educational Services* (Feb. 2014), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf (last visited August 27, 2026).

on Google's platform. None of these uses is necessary to deliver the homework-help service that the user requested from Defendant.

V. DEFENDANT ALLOWS SENSITIVE EDUCATIONAL INFORMATION TO BE INTERCEPTED ON ITS PLATFORM.

79. The data that Defendant transmits through Google Analytics is among the most sensitive that exists for a student—and is especially sensitive when, as is frequently the case here, the student is a minor.

80. The specific combination of fields captured by Google Analytics—persistent identifier, full text of the academic question submitted, event parameters describing the user's engagement, and session and device data—constitutes a comprehensive record of each user's educational use of the Platform.

81. That record discloses, at a minimum: (a) the specific subjects, courses, and academic levels at which the user is working; (b) the specific topics on which the user is unable to answer questions without outside assistance; (c) the personal context embedded in the user's questions, including, in many cases, the student's name, school, teacher, family circumstances, and the content of essays touching on the student's identity, mental health, and life circumstances; (d) the frequency and intensity of the user's reliance on the Platform; and (e) the user's inferred academic ability and rate of progress, derived from the difficulty of the material the user cannot complete without assistance.

82. Educational data—and particularly educational data about minors—is widely recognized as sensitive by federal regulators and government oversight bodies.

83. In a policy statement adopted unanimously on May 19, 2022, the Federal Trade Commission warned providers of education technology that children may not be required to submit to commercial surveillance and data monetization in

order to access educational services, and that an operator collecting student information may use that information only to provide the educational service requested—not for unrelated commercial purposes.[13]

84. The U.S. Government Accountability Office has likewise reported that when a student's personal information is disclosed, it "can lead to physical, emotional, and financial harm," and found that students' academic records were the most frequently compromised category of information across the reported K–12 data breaches it examined—58 of the 99 breaches analyzed.[14]

85. Disclosure of a user's educational queries to a data broker or advertising platform creates a durable record of that activity that can be sold, combined with other data sources, and used for purposes ranging from targeted advertising directed at minors, to the inference of cognitive ability or disability, to the construction of permanent behavioral profiles that follow the student into adulthood.

86. Moreover, the disclosure of Sensitive Educational Information to an advertising platform like Google creates a known risk of behaviorally targeted advertising directed at children and adolescents.

87. Every additional data point that Google receives about a student's academic struggles increases the scope and precision of Google's ability to target that student with advertising, predictive scoring, and other commercialized

[13] Fed. Trade Comm'n, *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act* (May 19, 2022), https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection (last visited August 27, 2026).

[14] U.S. Gov't Accountability Off., GAO-20-644, *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm* (Sept. 2020), https://www.gao.gov/products/gao-20-644 (last visited August 27, 2026).

inferences—including inferences about the student's intelligence, future prospects, and economic value as a target of advertising.

88. Defendant intercepted and transmitted users' communications with the Platform's AI to Google before any user had the opportunity to accept or decline that practice. Defendant structured the Platform so that the interception was already complete by the time a user could have acted on any description of it.

89. Defendant does not gate access to the Platform behind any privacy disclosure. No user is required to open, scroll through, or accept a privacy policy before submitting an academic question, and the Platform functions fully for users who never do. Rather, new users are induced to immediately enter their questions without any notice, constructive or otherwise, of Defendant's policies.

90. Prior to facilitating transmission of user questions, Defendant never notifies users of the Google Analytics tracking code on the Platform, and by the time a user could locate, open, and read anything Defendant makes available describing its data practices, the full text of that user's first academic question, together with the persistent identifier linking it to the user's device, has already been transmitted to Google.[15]

91. Whereas reasonable users would expect communications made on the Platform to remain private, and whereas the interception is complete before any user could act to prevent it, Defendant has allowed Google to intercept, in real time, every academic question submitted to the Platform and every page or screen view

[15] *See Gauth Privacy Policy, supra n.1*. Google's own Terms require website operators not only to disclose their use of Google Analytics, but also to provide users with a "prominent link" to Google's disclosure page explaining how Google uses information from sites or apps that use its services. *See Google Analytics Terms of Service*, https://marketingplatform.google.com/about/analytics/terms/us/ (last visited August 27, 2026).

associated with it, together with a persistent identifier that links that activity to the individual user.

92. Once received, Google does not merely store the intercepted data on Defendant's behalf or use it solely to provide services to Defendant.

93. Rather, Google uses the data intercepted from Defendant's Platform for its own independent commercial purposes, combining it with data collected from across the millions of other websites and applications that have integrated Google Analytics—and from Google's own consumer-facing services—to build and refine comprehensive, cross-platform user profiles that are then made available to third-party advertisers.

94. Users of the Platform never contemplated, consented to, or were informed that their Sensitive Educational Information would be used by Google for these independent commercial purposes—purposes wholly unrelated to the AI homework-help services Defendant provides.

95. Defendant did not obtain users' informed consent to the interception and transmission of their Sensitive Educational Information to Google. The absence of any disclosure to users is particularly significant because users of an AI homework-help service have a heightened expectation of privacy regarding their academic queries and educational activity, and because a substantial portion of those users are minors who cannot lawfully provide consent to commercial data-sharing under federal and state law.

REPRESENTATIVE PLAINTIFF'S EXPERIENCE.

96. Plaintiff Edward Lominchar currently resides (and at all times relevant hereto has resided) in Miami, Florida.

97. On or about December 2024, while living and physically present in Florida, and while a minor enrolled in high school, Plaintiff first used the Platform

through its website, without an account and without signing in, by entering academic questions into the Platform's question field and receiving AI-generated responses in return.

98. Plaintiff was not presented with Defendant's Privacy Policy prior to his first submission of a question to the Platform, nor was he required to click through, scroll past, or otherwise assent to any privacy disclosure, and did not read or view the Privacy Policy.

99. Only after Plaintiff had already used the Platform and submitted academic questions to it did Plaintiff register for an account.

100. Plaintiff thereafter continued to use the Platform's website on a regular basis through approximately January 2026.

101. During his use of the Platform, Plaintiff submitted to the Platform numerous academic questions, including questions concerning his high school coursework, drafts of personal essays, and other content reflecting his academic work and personal circumstances.

102. Plaintiff reasonably expected that the text of those questions would remain confidential between himself and Defendant for the purpose of generating an AI response.

103. Throughout Plaintiff's use of the Platform, the Google Analytics tracking code embedded within the Platform secretly intercepted Plaintiff's private communications with Defendant—including the full text of the academic questions Plaintiff submitted; the URLs and titles of the screens on which Plaintiff was working; Plaintiff's session and engagement data; Plaintiff's device identifiers (including the persistent Google Analytics client identifier); Plaintiff's IP address; and Plaintiff's browser information—and transmitted that information to Google without Plaintiff's knowledge or consent.

104. At no point before, during, or after using the Platform did Plaintiff consent to Plaintiff's Sensitive Educational Information, personal data, or device identifiers being intercepted and transmitted to Google as described herein.

105. Defendant's Privacy Policy did not notify Plaintiff that Plaintiff's interactions with the Platform would be shared with Google through the embedded Google Analytics tracking code, and Plaintiff was never presented with that disclosure or any other disclosure of that practice at any point before his use of the Platform.

106. When he began using the Platform, Plaintiff was unaware that his information was being captured in real time by the Google Analytics tracking code embedded within the Platform and disclosed to Google, which combines user data from across the web and mobile applications to create personalized, identifiable advertising profiles.

107. Had Plaintiff known that Defendant was using Google Analytics to capture Plaintiff's Sensitive Educational Information, including the full text of his academic questions, and that Google combines this data with users' broader digital activity to build personalized advertising profiles, Plaintiff would not have used the Platform, would have limited the information Plaintiff provided and the extent of Plaintiff's engagement, or would not have used the Platform on the terms offered.

108. As a direct and proximate result of Defendant's conduct, Plaintiff's privacy rights were violated, and Plaintiff suffered harm in the form of: the unauthorized disclosure of Plaintiff's Sensitive Educational Information to Google; the receipt of unwanted targeted advertisements across Plaintiff's other digital activity related to Plaintiff's use of the Platform; loss of control over Plaintiff's private personal data and Sensitive Educational Information; loss of the benefit of the bargain in keeping or exchanging Plaintiff's private data; and other harms related

to the undisclosed and non-consensual transmission of Plaintiff's Sensitive Educational Information.

TOLLING OF THE STATUTE OF LIMITATIONS

109. The applicable statutes of limitations are tolled as to Plaintiff and members of the Class on each of the following independent grounds.

110. *Minority.* Plaintiff was a minor when he first used the Platform and when the interceptions alleged herein began, and a substantial portion of the Class likewise consists of minors. Limitations periods do not run against a claimant during minority; under California law, for example, the period during which a claimant is under the age of majority "is not part of the time limited for the commencement of the action." Cal. Civ. Proc. Code § 352(a).

111. The limitations period as to Plaintiff and each minor Class member is therefore tolled until that person reaches the age of majority.

112. *Delayed discovery.* Plaintiff and Class members did not discover, and could not reasonably have discovered, Defendant's transmission of their Sensitive Educational Information to Google. The Google Analytics tracking code operates invisibly to the user; nothing Defendant presents to users identifies Google, discloses the existence of the tracking code, or discloses that the content of users' academic questions is transmitted to Google.

113. Discovery of the transmissions requires technical inspection of the Platform's network traffic, which no ordinary user—and no minor user—would undertake. Consistent with that reality, the ECPA's limitations period runs not from the date of interception but from "the date upon which the claimant first has a reasonable opportunity to discover the violation." 18 U.S.C. § 2520(e).

114. *Fraudulent concealment.* Defendant transmitted users' communications to Google while presenting users no disclosure of that practice at

any point before or during their use of the Platform. Defendant's concealment had the purpose and effect of preventing Plaintiff and Class members from learning of their claims. Defendant is therefore estopped from asserting any limitations defense, and any applicable limitations period is tolled until the concealment was or reasonably could have been discovered.

CLASS ACTION ALLEGATIONS

115. Plaintiff brings this action on behalf of himself and all others similarly situated pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3).

116. Plaintiff seeks to represent the following class:

> All persons in the United States who used the Platform at Gauth.ai or Gauthmath.com whose data was intercepted and transmitted to Google by the Google Analytics tracking code embedded in the Platform (the "Nationwide Class" or the "Class").

117. Excluded from the Class are Defendant, its officers, directors, employees, parents, subsidiaries, affiliates, and legal representatives; any entity in which Defendant has a controlling interest; the judge(s) presiding over this action and their immediate family members and staff; and all persons who have already received or are entitled to receive compensation for the same claims asserted herein.

118. **Numerosity:** The exact number of members of the Class is unknown but, upon information and good faith belief, is estimated to number in the millions, given that the Platform is one of the most widely used AI homework-help services in the United States and is used by students of all ages. Individual joinder of these claims is therefore wholly impracticable. Members of the Class can be readily identified through Defendant's records and objective criteria, and notice can be provided through techniques similar to those customarily used in other class action lawsuits.

119. **Typicality:** Plaintiff's claims are typical of the claims of other members of the Class in that Plaintiff and the members of the Class sustained damages arising out of Defendant's wrongful conduct, concealment, and unlawful practices, and Plaintiff and members of the Class sustained similar injuries and damages as a result of Defendant's uniform illegal conduct.

120. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with or are antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff.

121. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the Class and those questions predominate over any questions that may affect individual members of the Class. Common questions include, but are not limited to:

a. Whether Defendant embedded the Google Analytics tracking code within the Platform;

b. Whether the Google Analytics tracking code intercepted and transmitted users' Sensitive Educational Information—including the full text of academic questions and a persistent identifier—to Google;

c. Whether Defendant disclosed those transmissions to users or obtained users' consent;

d. Whether Defendant violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511, 2520;

e. Whether Defendant violated the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632;

f. Whether Defendant's conduct constitutes intrusion upon seclusion;

g. Whether Defendant's conduct constitutes an invasion of privacy;

h. Whether Defendant was unjustly enriched by transmiting and monetizing users' Sensitive Educational Information; and

i. Whether Plaintiff and Class members are entitled to damages and injunctive relief.

122. **Superiority:** There are substantial benefits to proceeding as a class action that render proceeding as a class action superior to any alternatives, including that class-wide adjudication will provide a realistic means for members of the Class to receive monetary relief; the monetary relief suffered by individual members of the Class may be relatively small; class adjudication would be substantially less burdensome on the courts and the parties than numerous individual proceedings; many members of the Class—particularly minors—may be unaware that they have equitable recourse for the conduct alleged herein; and issues common to members of the Class can be effectively managed in a single proceeding. Plaintiff and counsel know of no difficulty that could be encountered in the management of this litigation that would preclude its maintenance as a class action.

123. **Ascertainability:** Members of the Class are readily ascertainable through Defendant's own records, which include user account information (including names, email addresses, account-creation dates, and self-reported age or grade level) and server logs reflecting users' interactions with the Platform.

CAUSES OF ACTION

COUNT I

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. §§ 2511, 2520
(On Behalf of Plaintiff & the Nationwide Class)

124. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

125. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1)(a), prohibits any person from intentionally intercepting, endeavoring to

intercept, or procuring any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.

126. Plaintiff's and Class members' interactions with the Platform—including the full text of the academic questions they submitted, the searches they ran, the screens they viewed, and the engagement data associated with those interactions—constitute "electronic communications" within the meaning of 18 U.S.C. § 2510(12) because they are transfers of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system.

127. Defendant intentionally embedded the Google Analytics tracking code within the Platform, which intercepted Plaintiff's and Class members' electronic communications and transmitted the contents of those communications—including the full text of the academic questions submitted to the Platform's AI for assistance—to Google in real time, simultaneously with the transmission of those communications between users and Defendant, and without the knowledge or consent of Plaintiff or the Class members.

128. While 18 U.S.C. § 2511(2)(d) provides an exception permitting a party to a communication to intercept that communication, this exception expressly does not apply where the communication is intercepted "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."

129. Defendant's facilitation of the interception of Plaintiff's and Class members' electronic communications was undertaken for the purpose of committing tortious acts in violation of the common law and the laws of the several States—specifically, the common-law torts of invasion of privacy and intrusion upon seclusion, as alleged in Counts IV and V below, arising from Defendant's intentional

and highly offensive intrusion into Plaintiff's and Class members' private affairs, and the processing and profiling of the personal information of consumers under eighteen years of age restricted by Fla. Stat. § 501.1735(2) and by the parallel provisions of the laws of the several States in which Class members reside, including Colo. Rev. Stat. § 6-1-1308.5; Md. Code Ann., Com. Law § 14-4607; Conn. Gen. Stat. §§ 42-515, *et seq*.; N.Y. Gen. Bus. Law §§ 899-ff, *et seq*.; Cal. Civ. Code § 1798.120(c); and Tex. Bus. & Com. Code §§ 509.001, *et seq*.

130. Specifically, Defendant embedded the Google Analytics tracking code within the Platform to intercept users' Sensitive Educational Information, including the precise academic questions users submitted to the Platform's AI, and to transmit that data—together with a persistent identifier capable of linking it to an identifiable minor—to Google for advertising, analytics, and cross-property profiling purposes wholly unrelated to the delivery of the homework-help service the user requested.

131. In any event, Google, in receiving the intercepted communications, acts not as a mere conduit for Defendant but as an independent third-party interceptor for its own commercial purposes.

132. Defendant's conduct was willful and intentional.

133. Defendant deliberately implemented the Google Analytics tracking code knowing it would intercept users' electronic communications and transmit them to Google without proper consent, and without first presenting users with any disclosure of that practice before or during their use of the Platform.

134. As a direct and proximate result of Defendant's violations of 18 U.S.C. § 2511, Plaintiff and the Class members have been injured and are entitled to relief pursuant to 18 U.S.C. § 2520, including: (a) statutory damages of the greater of $100 per day of violation or $10,000 for each Class member; (b) punitive damages in appropriate cases; (c) a reasonable attorney's fee and other litigation costs

reasonably incurred; and (d) such preliminary and other equitable or declaratory relief as may be appropriate.

COUNT II

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT

Cal. Penal Code § 631

(On Behalf of Plaintiff & the Nationwide Class)

135. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

136. Plaintiff brings this claim individually and on behalf of the members of the Nationwide Class.

137. California Penal Code § 631(a) establishes liability for any person who:

> [I]ntentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> Or
>
> [W]illfully 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
>
> [U]ses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> Or
>
> [A]ids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

138. At all relevant times, Plaintiff and Nationwide Class members were accessing and using the Platform to obtain assistance with their academic work. Plaintiff's and Nationwide Class members' interactions with the Platform constitute communications in transit over a wire, line, cable, or instrument within the meaning of Cal. Penal Code § 631(a).

139. The Google Analytics tracking code embedded within the Platform constitutes an unauthorized connection to a wire, line, cable, or instrument and is a device capable of intercepting communications within the meaning of Cal. Penal Code § 631, as it is specifically designed to capture, copy, and transmit user communications as they occur and while they are in transit between the user's device and Defendant's servers.

140. Defendant aided, agreed with, employed, and conspired with Google to intercept Plaintiff's and Nationwide Class members' communications by embedding the Google Analytics tracking code within the Platform and by configuring that tracking code to transmit users' Sensitive Educational Information to Google for Google's own use.

141. Google, in turn, willfully and without the consent of all parties to the communications read and learned the contents of Plaintiff's and Nationwide Class members' communications with Defendant while those communications were in transit and used the information so obtained for its own independent commercial purposes, including advertising, audience building, and cross-platform profiling.

142. Defendant's procurement of Google's interception, was accomplished without the consent of Plaintiff or the Nationwide Class members. Specifically:

a. Defendant never obtained express or implied consent from Plaintiff or Nationwide Class members before implementing the Google Analytics tracking code;

b. The Google Analytics tracking code begins transmitting user data to Google from the moment a user loads any page or screen of the Platform, before the user has had any opportunity to review the Privacy Policy or to provide informed consent;

c. Defendant never provided clear, conspicuous notice that users' Sensitive Educational Information—including the full text of the questions they submit—would be intercepted and shared with Google;

d. Nothing Defendant presents to users discloses the existence of the Google Analytics tracking code on the Platform or identifies Google by name, and no privacy disclosure is presented to users before they submit academic questions to the Platform; and

e. Any purported consent was ineffective because the interception began before consent could be obtained, because Defendant presented no disclosure to users before the interception began, and because a substantial portion of users are minors who cannot lawfully provide consent to commercial data-sharing under federal and state law.

143. The intercepted communications include highly sensitive information—the full text of academic questions, the subjects and grade level at which the user is working, personal context embedded in the user's questions, and the user's patterns of academic assistance-seeking—that Plaintiff and Nationwide Class members provided with reasonable expectations of privacy and confidentiality.

144. Defendant's conduct was willful and intentional, as Defendant deliberately implemented the Google Analytics tracking code knowing it would intercept users' electronic communications and transmit them to Google without proper consent.

145. As a direct and proximate result of Defendant's violations of Cal. Penal Code § 631, Plaintiff and Nationwide Class members have suffered injury, including invasion of privacy, loss of confidentiality of personal information, loss of control over their Sensitive Educational Information, and violation of their statutory rights.

146. Plaintiff and Nationwide Class members continue to desire to use the Platform's services but have a reasonable fear that their communications will continue to be intercepted without consent if they continue to do so.

147. Under Cal. Penal Code § 637.2, Plaintiff and Nationwide Class members are entitled to:

a. Five thousand dollars ($5,000) per violation;

b. Three times the amount of actual damages sustained by the Plaintiff and Nationwide Class members; and

c. Equitable or declaratory relief, including a preliminary and permanent injunction prohibiting Defendant from continuing its unlawful transmission of user communications.

COUNT III
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 632
(On Behalf of Plaintiff & the Nationwide Class)

148. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

149. Plaintiff brings this claim individually and on behalf of the members of the Nationwide Class.

150. California Penal Code § 632(a) provides that:

> [E]very 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[.]

151. California Penal Code § 632(c) defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, or other public proceeding in which the public is entitled to attend, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded."

152. The communications between Plaintiff and Nationwide Class members and Defendant through the Platform—and in particular the academic questions submitted to the Platform's AI—constitute "confidential communications" within the meaning of Section 632(c).

153. Plaintiff and Nationwide Class members had an objectively reasonable expectation of privacy with respect to those communications, and Defendant created and reinforced the reasonable expectation that users' Sensitive Educational Information is not shared with third parties like Google by (a) designing the Platform so that users may submit academic questions immediately, without an account and without encountering any privacy disclosure; (b) presenting no notice, interstitial, or consent screen advising users that their communications would be routed to any third party; (c) holding the Platform out as a private exchange between the user and Defendant's AI for the purpose of generating an answer; and (d) not disclosing the presence of the Google Analytics tracking code on the Platform.

154. Defendant intentionally used an electronic recording device—specifically, the Google Analytics tracking code embedded within the Platform—to eavesdrop upon and record these confidential communications.

155. The Google Analytics tracking code constitutes an "electronic amplifying or recording device" within the meaning of Section 632(a) because it is

specifically designed to capture, record, and transmit user interactions and communications in real time for analytics and behavioral-tracking purposes.

156. Defendant intentionally implemented and activated this recording technology within the Platform with full knowledge that it would capture and record users' confidential communications.

157. Defendant's recording of Plaintiff's and Nationwide Class members' confidential communications was accomplished without the consent of all parties to the communication, specifically:

a. Plaintiff and Nationwide Class members never consented to having their confidential communications recorded by the Google Analytics tracking code;

b. Defendant never obtained express consent before implementing the recording technology;

c. Users were not informed that their communications—including the full text of the academic questions they submit to the Platform's AI—would be recorded and transmitted to Google;

d. No clear, conspicuous notice was provided regarding the scope and nature of the recording of confidential communications; and

e. The recording began immediately upon loading the Platform, before users had any opportunity to review the Privacy Policy or to provide informed consent—and many users, as minors, could not have provided lawful consent in any event.

158. Defendant's conduct was undertaken intentionally and with knowledge that the Google Analytics tracking code would record confidential communications without proper consent from all parties.

159. The confidential communications that were unlawfully recorded include the full text of the academic questions Plaintiff and Nationwide Class members submitted to the Platform's AI, the subjects and content the users were

working on, and the personal context embedded in those questions—information that reveals the educational activities, abilities, and personal circumstances of Plaintiff and Nationwide Class members and the nature of their academic work.

160. As a direct and proximate result of Defendant's violations of Section 632, Plaintiff and Nationwide Class members have suffered harm, including invasion of their privacy rights, violation of confidentiality, and loss of control over their Sensitive Educational Information.

161. Unless enjoined and restrained by this Court, Defendant will continue to commit these violations. Plaintiff and Nationwide Class members have a reasonable fear that their confidential communications will continue to be unlawfully recorded if they continue to use the Platform.

162. Pursuant to California Penal Code § 637.2, Plaintiff and Nationwide Class members are entitled to:

a. A preliminary and permanent injunction prohibiting Defendant from continuing its unlawful recording of confidential communications;

b. Statutory damages of $5,000 per violation;

c. Three times the amount of actual damages, if any, sustained by Plaintiff and Nationwide Class members; and

d. Any other relief the Court deems proper.

COUNT IV
INTRUSION UPON SECLUSION
(On Behalf of Plaintiff & the Nationwide Class)

163. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

164. Under the Restatement (Second) of Torts § 652B, one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or her

private affairs or concerns, is subject to liability to the other for invasion of her privacy, if the intrusion would be highly offensive to a reasonable person.

165. Plaintiff and Class members had a reasonable expectation of privacy in their interactions with the Platform.

166. The Platform is designed for a deeply personal activity—the seeking of help with academic work, including (for many users) work assigned by their schools—that carries significant educational, reputational, and developmental implications. Users reasonably expected that the questions they submitted to the Platform's AI would remain between themselves and Defendant for the limited purpose of generating an AI response and would not be secretly intercepted and transmitted to a third-party advertising company.

167. Defendant reinforced this reasonable expectation of privacy by designing the Platform as a closed exchange: the user submits a problem, Defendant's AI returns a solution, and the interface presents the transaction as one occurring solely between the user and Defendant for the purpose of answering the question posed.

168. Defendant intentionally intruded upon the solitude and seclusion of Plaintiff and Class members by secretly embedding the Google Analytics tracking code within the Platform and configuring it to intercept users' private Sensitive Educational Information—including the full text of the academic questions users submitted, the subjects and grade levels at which users were working, and the personal context embedded in users' questions—and to transmit that data, alongside a persistent unique identifier, to Google in real time, without users' knowledge or consent.

169. The intrusion was into a matter that Plaintiff and Class members had a right to keep private. The categories of information intercepted—the academic

queries of students, including in many cases minors; the personal context embedded in those queries; and a comprehensive record of the user's reliance on outside assistance—constitute information whose disclosure can result in material educational, reputational, and developmental harm, including academic discipline, distortion of educational opportunity, exposure to age-inappropriate advertising, and the construction of permanent commercial profiles concerning a child's intellectual abilities and struggles.

170. Defendant's intrusion would be highly offensive to a reasonable person.

171. The following factors, considered together, establish the highly offensive nature of Defendant's conduct:

a. *The sensitivity of the information intercepted.* The data at issue concerns users' educational queries, abilities, and personal academic struggles. A substantial portion of users are minors, whose personal information Florida, Colorado, Maryland, Connecticut, New York, California, and Texas each protect from undisclosed profiling and from exploitation for targeted advertising, see Fla. Stat. § 501.1735; Colo. Rev. Stat. § 6-1-1308.5; Md. Code Ann., Com. Law § 14-4607; Conn. Gen. Stat. §§ 42-515, et seq.; N.Y. Gen. Bus. Law §§ 899-ff, et seq.; Cal. Civ. Code § 1798.120(c); Tex. Bus. & Com. Code §§ 509.001, et seq., and whose unique identifiers Florida law treats as protected personal information. *See* Fla. Stat. § 501.1735.

b. *The context of the intrusion.* Users engaged with the Platform in the expectation that they were communicating privately with an AI homework-help service—not broadcasting the details of their academic difficulties to the world's largest advertising company. The Platform invited users (including, by design, minor users) to disclose academic content and personal context; Defendant exploited that trust by diverting those communications to Google.

c. *The concealed means of intrusion.* Defendant did not merely fail to disclose the interception; it structured the Platform so that the interception began before a user could encounter any privacy disclosure at all. Users—especially minor users—had no reasonable means of discovering the embedded Google Analytics tracking code or the data transmissions without conducting a technical analysis of the Platform's network traffic.

d. *The scope and persistence of the intrusion.* The Google Analytics tracking code intercepted user data continuously—from the moment a user loaded any page or screen of the Platform and throughout every subsequent session—thereby capturing a comprehensive record of each user's

educational use of the Platform, including the full text of every academic question submitted.

e. *The independent commercial exploitation of the intercepted data.* Google did not merely receive and store the data on Defendant's behalf but incorporated the intercepted communications into its own advertising ecosystem, thereby creating detailed, cross-platform behavioral profiles of individual users—including minors—which were then made available to unrelated third-party advertisers for targeted advertising, retargeting, and campaign optimization.

172. Defendant's intrusion was intentional. Defendant made a deliberate business decision to embed the Google Analytics tracking code within the Platform, to configure it to capture users' private communications (including the full text of users' academic questions), and to enable the transmission of that data to Google for advertising and analytics purposes—and to do so without regard to whether the user was a minor whose personal information Florida law treats as protected.

173. As a direct and proximate result of Defendant's intrusion upon the seclusion of Plaintiff and Class members, Plaintiff and Class members have suffered damages, including but not limited to loss of privacy, loss of control over their Sensitive Educational Information, the unauthorized construction of advertising profiles incorporating their private communications, the receipt of targeted advertisements derived from their intercepted personal data, and anxiety and emotional distress regarding the unauthorized disclosure of their Sensitive Educational Information.

COUNT V

INVASION OF PRIVACY

(On Behalf of Plaintiff & the Nationwide Class)

174. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

175. Plaintiff and Class members had a reasonable expectation of privacy in their Sensitive Educational Information the Platform, which they used to obtain

assistance with their academic work.

176. Defendant intentionally intruded upon the private affairs of Plaintiff and Class members by secretly embedding the Google Analytics tracking code within the Platform, which intercepted and transmitted users' Sensitive Educational Information—including the full text of the academic questions users submitted—to Google without their knowledge or consent.

177. Defendant's intrusion into the private affairs of Plaintiff and the Class would be highly offensive to a reasonable person.

178. Users of an AI homework-help service—especially when, as here, a substantial portion of those users are minors—have a heightened expectation that their activities within that service, including the academic questions they submit for AI assistance, will remain private.

179. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and Class members have suffered damages, including but not limited to the loss of privacy and the unauthorized disclosure of their private information.

COUNT VI

UNJUST ENRICHMENT

(On Behalf of Plaintiff & the Nationwide Class)

180. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

181. Plaintiff pleads this claim in the alternative to the foregoing counts.

182. Defendant received a benefit from Plaintiff and Class members in the form of their Sensitive Educational Information, which Defendant transmitted to Google, and in exchange for which Defendant received advertising-related revenue, analytics services, and other valuable consideration from Google.

183. Defendant's retention of the benefits conferred by Plaintiff and Class members—namely their Sensitive Educational Information—is inequitable and

unjust because Defendant obtained those benefits through the secret interception and transmission of users' private communications without their knowledge or consent, and without ever presenting users with any disclosure of that practice.

184. Plaintiff and Class members are entitled to disgorgement of the revenues and profits Defendant obtained as a result of its unjust enrichment.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Edward Lominchar, individually and on behalf of the Class, respectfully requests that this Court enter judgment against Defendant TikTok USDS Joint Venture, LLC and award the following relief:

A. An order certifying the Class as defined herein, appointing Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Statutory damages under the ECPA, 18 U.S.C. § 2520(c)(2), of the greater of $100 per day of violation or $10,000 for each Class member, plus punitive damages;

C. Statutory damages under CIPA, Cal. Penal Code § 637.2(a), of $5,000 per violation for each Nationwide Class member, and treble damages for any actual damages sustained;

D. Compensatory and consequential damages in an amount to be determined at trial;

E. Disgorgement of Defendant's ill-gotten revenues and profits;

F. Injunctive relief requiring Defendant to cease the unauthorized interception and transmission of users' data to Google, with heightened protections for minor users consistent with Fla. Stat. § 501.1735;

G. Pre-judgment and post-judgment interest as allowed by law;

H. Reasonable attorney's fees and litigation costs pursuant to 18 U.S.C. § 2520(b)(3), Cal. Penal Code § 637.2, and any other applicable statute; and

I. Such other and further relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the Class, hereby demands a trial by jury on all issues so triable.

Dated: August 31, 2026

Respectfully Submitted,

/s/ Victor J. Sandoval
Victor J. Sandoval (SBN 344461)
ALMEIDA LAW GROUP LLC
3415 S. Sepulveda Blvd., Suite 1121
Los Angeles, California 90034
Telephone: (562) 534-5907
victor@almeidalawgroup.com

Attorney for Plaintiff & the Putative Class