UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

TINA ZEOLLA and **KIRSTEN KELLOGG**, on behalf of themselves and all others similarly situated, Plaintiffs, v. **SOUTHERN NEW HAMPSHIRE UNIVERSITY**, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Tina Zeolla and Kirsten Kellogg (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendant Southern New Hampshire University ("SNHU" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. It is easy to understand why students highly value the confidentiality of their education records, particularly where it comes to their financial aid needs, grades and GPAs.

2. As such, it is not surprising that both state and federal law have long required that educational institutions must protect the confidentiality of their students' information, including through the Federal Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, *et seq*., which prohibits any regulated entity from disclosing personally identifiable education records to an unauthorized third party.

3. SNHU is a "private, nonprofit, accredited institution with more than 3,000 on campus students and over 200,000 online students, making it one of the fastest growing universities in the nation."[1]

4. SNHU's students are required to use mySNHU, Defendant's online student portal. Using mySNHU, students can review their grades, enroll in courses, apply for financial aid, pay their tuition bills, and access their SNHU e-mail accounts.[2] Each of the Plaintiffs enrolled as SNHU students and used mySNHU for some or all of these purposes, as described more fully below.

5. Unfortunately, unbeknownst to Plaintiffs and other SNHU students, Defendant does not keep its student's private academic information confidential. Instead, through mySNHU, Defendant collected and transmitted a substantial amount of sensitive, personally identifiable information from Plaintiffs' and Class Members' education records to unauthorized third parties, including Alphabet, Inc. ("Google") and ByteDance, Inc. ("TikTok"), through the use of surreptitious online tracking tools.

6. The information that SNHU transmitted included a shocking amount of highly confidential information, such as Plaintiffs' and Class Members':

a. full names;
b. e-mail addresses;
c. phone numbers;
d. addresses;
e. ethnicities;
f. gender identities;
g. career statuses;
h. SNHU student ID numbers;
i. whether they have served in the military;
j. whether they are a first-generation college student;
k. whether they have applied for financial aid;
l. detailed descriptions of **every** course in which they have enrolled; and

[1] *About Us*, SNHU, https://www.snhu.edu/about-us (last accessed Dec. 2, 2025).
[2] *Accepted Students*, SNHU, https://campus.snhu.edu/admission/accepted-students (last accessed Dec. 2, 2025).

m. their cumulative GPAs

(collectively, the "Sensitive Information").

7. Why an educational institution like SNHU would choose to disclose this vast trove of private information is simple: to help the university market itself and grow its student base. Online advertising giants like Google and TikTok are hungry to accumulate as much information as possible about American consumers, including information relating to the most private aspects of their lives. This information then serves as the fuel for their massive, targeted advertising enterprise because any information about a person captured by those online behemoths can be used to stream ads to that person.

8. Obviously, platforms like Google and TikTok track their own users, but they have also developed a system to track users on other websites as well. Those companies offer website operators access to their proprietary suites of marketing, advertising, and customer analytics software, including Google Analytics, Google AdSense, Google Tag Manager, and TikTok Pixel (collectively, the "Business Tools"). Armed with these Business Tools, website operators can leverage Google and TikTok's enormous database of consumer information for the purposes of deploying targeted advertisements, performing minute analyses of their customer bases, and identifying new market segments that may be exploited.

9. In exchange for access to these Business Tools, website operators install Google and TikTok's surveillance software on their websites (the "Tracking Tools"), including 'tracking pixels' ("Pixels") and third-party 'cookies' that capture sensitive, personally identifiable information provided to the website operator by its website users. This sensitive information can include a unique identifier that Google and TikTok use to identify that user, regardless of what computer or phone is used to access the website. The Tracking Tools can also capture and share

other information like the specific webpages visited by a website user, items added to an online shopping cart by a website user, information entered into an online form by a website user, and the device characteristics of a website user's phone or computer.

10. In essence, when website operators use Google and TikTok's Business Tools, they choose to participate in Google and TikTok's mass surveillance network and, in turn, benefit from Google and TikTok's collection of user data at the expense of their customers' privacy.

11. As is clear from the surprising amount of information that SNHU shares, it clearly has chosen to prioritize its marketing efforts and profits over its students' privacy by installing the Tracking Tools on its website. Each of the Plaintiffs and Class Members used mySNHU and had their personal Sensitive Information tracked by Defendant using the Tracking Tools. Defendant ***never*** obtained authorization from Plaintiffs or Class Members to share their Sensitive Information with third parties. Therefore, at all relevant times, Plaintiffs and Class Members could not, and did not, provide informed consent for their Sensitive Information to be transmitted to the third parties, including to the largest advertisers and compilers of personal information in the world.

12. Not only does this massive disclosure of information breach Plaintiffs' and Class Members' reasonable expectations of privacy, but it constitutes a serious violation of FERPA and other state laws.

13. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with educational providers; (iii) emotional distress and heightened concerns related to the release of Sensitive Information to third parties, (iv) loss of benefit of the bargain; (v) diminution of value of the Sensitive Information; (vi) statutory damages and (vii) continued and ongoing risk to their Sensitive Information.

14. Therefore, Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and assert the following statutory and common law claims against Defendant: Invasion of Privacy; Negligence; Breach of Implied Contract; Unjust Enrichment; Violations of the New Hampshire Wiretap Act, N.H. Rev. Stat. § 570-A, *et seq.*; and violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq*.

II. PARTIES

Plaintiff Tina Zeolla

15. Plaintiff Zeolla is a citizen of the State of Massachusetts, residing in Norfolk County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

16. Plaintiff Zeolla is currently enrolled at SNHU, and routinely uses mySNHU in the manner depicted in §IV(A)(iv), *infra*.

17. Unbeknownst to Plaintiff Zeolla, Defendant transmitted her Sensitive Information to unauthorized third parties through the Tracking Tools.

18. Plaintiff Zeolla never authorized Defendant to disclose any part of her student records, or other information provided to Defendant through mySNHU.

19. On every occasion that she used mySNHU, Plaintiff Zeolla possessed an account with Google, and she accessed mySNHU while logged into her Google account on the same device.

Plaintiff Kerstin Kellogg

20. Plaintiff Kellogg is a citizen of the State of Michigan, residing in Saginaw County and brings this action both in an individual capacity, and on behalf of all others similarly situated.

21. Plaintiff Kellogg was enrolled with SNHU until December of 2025, and routinely used mySNHU in the manner depicted in §IV(A)(iv), *infra* during her time as a student.

22. Unbeknownst to Plaintiff Kellogg, Defendant transmitted her Sensitive Information to unauthorized third parties through the Tracking Tools.

23. Plaintiff Kellogg never authorized Defendant to disclose any part of her student records, or other information provided to Defendant through mySNHU.

24. On every occasion that she used mySNHU, Plaintiff Kellogg possessed an account with Google, and she accessed mySNHU while logged into her Google account on the same device.

Defendant SNHU

25. Southern New Hampshire University is an accredited private university, with its principal place of business located at 2500 North River Road, Manchester, NH, in Hillsborough County.

III. JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than Defendant. Additionally, this Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this Complaint asserts a claim for violation of federal law, specifically, the ECPA, 18 U.S.C. § 2511. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

27. This Court has personal jurisdiction over Defendant because it is headquartered in this judicial district, and has otherwise made or established contacts in the State of New Hampshire and in this judicial district sufficient to permit the exercise of personal jurisdiction.

28. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims in this action occurred in this judicial district.

IV. FACTUAL ALLEGATIONS

A. DEFENDANT'S USE OF THIRD-PARTY TRACKING TECHNOLOGIES

i. The Google and TikTok Mass Advertising Surveillance Operations

29. Google is the largest digital advertiser in the country, accounting for 26.8-percent of the total digital advertising revenue generated in the United States.[3] In 2023, Google's advertising revenue of $238 billion accounted for 77-percent of its total revenue for the year.[4]

30. Google advertises Google Analytics and other Business Tools to website operators, like Defendant, claiming they will allow the operator to "[u]nderstand [their] site and app users," "check the performance of [their] marketing," and "[g]et insights only Google can give."[5] But, in order for website operators to get information from Google Analytics about their website's visitors, they must allow data collection through installation of Google's Tracking Tools on their website.[6]

31. Indeed, on its *Privacy & Terms* page, Google admits that it collects information from third party websites, stating that: "[m]any websites and apps use Google services to improve

---

[3] *Share of major ad-selling companies in digital advertising revenue in the United States*, STATISTA (May 2024), https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/#:~:text=In%202023%2C%20Google%20accounted%20for,21.1%20and%2012.5%20percent%2C%20respectively https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/ (last accessed Oct. 23, 2025).

[4] Florian Zandt, *Google's Ad Revenue Dwarfs Competitors*, STATISTA (Sep. 10, 2024), https://www.statista.com/chart/33017/annual-advertising-revenue-of-selected-tech-companies-offering-search-solutions/#:~:text=Online%20advertising&text=Alphabet%2C%20the%20company%20behind%20the,overall%20revenue%20this%20past%20year (last accessed Oct. 23, 2025).

[5] *Welcome to Google Analytics*, GOOGLE, https://analytics.google.com/analytics/web/provision/?authuser=0#/provision (last accessed Oct. 23, 2025).

[6] *See* Aaron Ankin & Surya Matta, *The High Privacy Cost of a "Free" Website*, THE MARKUP, https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites (last accessed Oct. 23, 2025).

their content and keep it free. When they integrate our services, these sites and apps share information with Google."[7]

32. Google also admits that it uses the information collected from third party websites, such as mySNHU, to sell targeted advertising, explaining to users that: "[f]or example, a website that sells mountain bikes might use Google's ad services. After you visit that site, you could see an ad for mountain bikes on a different site that shows ads served by Google."[8]

33. TikTok is a social media company that allows users to share and watch short-term video content, subscribe to other TikTok users, and find videos and content creators relevant to their interests. While TikTok is a newer entrant to the online advertising industry, it has grown rapidly, with its global ad revenue estimated to surpass $32-billion this year.[9]

34. TikTok admits that it will "match" the information collected through its Tracking Tools with "corresponding accounts on TikTok inventory to create a subset of matched IDs …and combine those Matched IDs with corresponding" data collected from other website operators and through its products.[10]

35. While Google and TikTok admit that they collect information from third-party websites through the Tracking Tools, neither provides, nor could provide, a publicly available list of every webpage on which their Tracking Tools are installed. As such, the vague descriptions of Google and TikTok's data collection practices referenced above could not give Plaintiffs and Class

---

[7] *Privacy & Terms – How Google uses information from sites or apps that use our services*, GOOGLE, https://policies.google.com/technologies/partner-sites (last accessed Oct. 23, 2025).

[8] *Id*.

[9] *Platform Insights: TikTok 2025*, WARC (Mar. 4, 2025), *available online at*: https://www.warc.com/content/paywall/article/Warc-Data/Platform_Insights_TikTok_2025/en-GB/159437?.

[10] *TikTok Business Products (Data) Terms*, TIKTOK (July 29, 2024), *available online at*: https://ads.tiktok.com/i18n/official/policy/business-products-terms.

Members any reason to think that Defendant was part of Google and TikTok's surveillance networks. Moreover, as Defendant does not disclose its use of the Tracking Tools, Plaintiffs and Class Members could not have been reasonably expected to review any of Google and TikTok privacy statements in connection with their use of mySNHU.

36. Google and TikTok aggregate the user information that they collect from third-party websites into 'advertising profiles' consisting of all of the data that they have collected about a given user.[11] With these advertising profiles, Google and TikTok can sell hyper-precise advertising services, allowing their clients to target internet users based on combinations of their location, age, race, interests, hobbies, life events (e.g., recent marriages, graduation, or relocation), political affiliation, education level, home ownership status, marital status, household income, type of employment, use of specific apps or websites, and more.[12]

37. The surveillance of individuals' internet usage through Tracking Tools is ubiquitous. In 2017, Scientific American reported that over 70-percent of smartphone apps report "personal data to third-party tracking companies like Google[.]"[13] Google trackers are present on 74-percent of all web traffic.[14]

---

[11] Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (2019), *available online at*: https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf.

[12] *About audience segments*, GOOGLE ADS, https://support.google.com/google-ads/answer/2497941?hl=en#zippy=%2Cin-market-segments%2Caffinity-segments%2Clife-events%2Cdetailed-demographics ((last accessed Oct. 23, 2025); *About Ad Targeting in TikTok Ads Manager*, TIKTOK, https://ads.tiktok.com/help/article/ad-targeting?lang=en (last accessed Oct. 23, 2025).

[13] Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, SCIENTIFIC AMERICAN (May 30, 2017), https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/ (last accessed Oct. 23, 2025).

[14] *WhoTracksMe*, Ghostery, https://www.ghostery.com/whotracksme/ (last accessed Oct. 23, 2025).

38. Moreover, as in this case, the data collected through the Tracking Tools often pertains to the most personal and sensitive aspects of an individual's life. For example:

a. 93-percent of pornography websites allow third parties, including Google, to collect their user's browsing habits.[15] In fact, Google advertising trackers were found on 73-percent of pornography websites.[16]

b. 81-percent of the most popular mobile apps for managing depression and quitting smoking allowed Facebook and/or Google to access subscriber information, including health diary entries and self-reports about substance abuse.[17]

c. Twelve of the largest pharmacy providers in the United States send information regarding user's purchases of products such as pregnancy tests, HIV tests, prenatal vitamins, and Plan B to online advertisers.[18] For example, when an online shopper searches for a pregnancy test, views the product page for a pregnancy test, or adds a pregnancy test to their online shopping cart on Kroger's website, that information is transmitted to Google.[19]

39. This monumental, invasive surveillance of Americans' internet usage is not accidental. As Google's then-CEO Eric Schmit admitted in 2010: "We know where you are. We know where you've been. We can more or less know what you're thinking about."[20]

---

[15] Elena Maris, Timothy Libert & Jennifer R. Henrichsen, *Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites*, NEW MEDIA & SOCIETY (2020), *available online at*: https://journals.sagepub.com/doi/10.1177/1461444820924632.

[16] *Id*.

[17] Kit Huckvale, John Torous & Mark E. Larsen, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation*, JAMA NETWORK OPEN (2019), *available online at*: https://pubmed.ncbi.nlm.nih.gov/31002321/.

[18] Darius Tahir & Simon Fondrie-Teitler, *Need to Get Plan B or an HIV Test Online? Facebook May Know About It*, THE MARKUP (June 30, 2023), https://themarkup.org/pixel-hunt/2023/06/30/need-to-get-plan-b-or-an-hiv-test-online-facebook-may-know-about-it (last accessed Oct. 23, 2025).

[19] Jon Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You*, THE MARKUP (Feb. 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you (last accessed Oct. 23, 2025).

[20] Andrew Orlowski, *Google's Schmidt: We know what you're thinking*, THE REGISTER (Oct. 4, 2020), https://www.theregister.com/2010/10/04/google_ericisms/ (last accessed Oct. 23, 2025).

40. In fact, Google and TikTok value user information so highly that they provide their Business Tools to many website operators for free, all to expand their surveillance apparatus.[21]

41. When website operators, like Defendant, make use of Google and TikTok's Business Tools, they are essentially choosing to participate in Google and TikTok's mass surveillance network, and in return they benefit from Google and TikTok's collection of user data, at the expense of their website users' privacy. For example, Google rewards website operators for providing it with their user's information by granting access to its Analytics platform, which leverages demographic data collected by Google to provide detailed analyses of the website's user base.[22] TikTok's advertising platform similarly allows website operators to retarget prior visitors, measure their ad performance, and analyze their website audience if the website operator installs the TikTok Pixel.[23]

42. In many cases, a website operator's use of third-party tracking software is not disclosed whatsoever in its privacy policy.[24] Even where the use of such third-party software is disclosed, such disclosures are often hidden and cloaked in such confusing, technical and overly legal language as to be indecipherable to the typical internet user.[25]

43. Moreover, for even a conscientious internet user, the massive volume of privacy policies encountered through routine internet use makes reviewing each and every one practically

---

[21] *Analytics Overview*, GOOGLE, https://marketingplatform.google.com/about/analytics/ ((last accessed Oct. 23, 2025) ("Google Analytics gives you the tools, free of charge"); *Get started with the TikTok Pixel*, TIKTOK (Sep. 6, 2024), https://ads.tiktok.com/business/en-US/blog/get-started-with-tiktok-pixel (last accessed Oct. 23, 2025) ("Bonus: it's free").

[22] *Google Marketing Platform – Features*, GOOGLE, https://marketingplatform.google.com/about/analytics/features/ (last accessed Oct. 23, 2025).

[23] *Get started with the TikTok Pixel*, TIKTOK (Sep. 6, 2024), https://ads.tiktok.com/business/en-US/blog/get-started-with-tiktok-pixel (last accessed Oct. 23, 2025).

[24] *See* Woodrow Hartzog, *Privacy's Blueprint*, 60-67 (Harvard University Press 2018) (detailing deficiencies with online privacy policies).

[25] *Id*.

impossible. According to one study, it would take the average internet user 244 hours – or 30.5 working days – to read the privacy policy of every new website that they visited in a single year.[26]

ii. Pixels Can Record Almost Every Interaction Between a User and a Website

44. In order to use Google and TikTok's Business Tools, Defendant installed the Tracking Tools, including tracking Pixels, onto mySNHU.

45. Pixels are one of the tools used by website operators to track user behavior. As the Federal Trade Commission ("FTC") explains, a Pixel is:

> [A] small piece of code that will be placed into the website or ad and define [the Pixel operator's] tracking goals such as purchases, clicks, or pageviews…
>
> Pixel tracking can be monetized several ways. One way to monetize pixel tracking is for companies to use the tracking data collected to improve the company's own marketing campaigns…Another is that companies can monetize the data collected by further optimizing their own ad targeting systems and charging other companies to use its advertising offerings.[27]

46. Pixels can collect a shocking amount of information regarding an individual's online behavior, including the webpages viewed by the user, the amount of time spent by the user on specific webpages, the specific buttons and hyperlinks that the user clicks, the items that the user adds to an online shopping cart, the purchases that a user makes through an online retailer, the text entered by the user into a website search bar, and even the information provided by the user on an online form.[28]

---

[26] Aleecia M. McDonald & Lorrie Faith Cantor, *The Cost of Reading Privacy Policies*, I/S: A JOURNAL OF LAW AND POL. FOR THE INFO. SOC. (2008), *available online at*: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[27] *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FEDERAL TRADE COMMISSION – OFFICE OF TECHNOLOGY (Mar. 6, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking (last accessed Oct. 23, 2025).

[28] *See id.*; Tom Kemp, *"Oops! I Did It Again" … Meta Pixel Still Hoovering Up Our Sensitive Data*, MEDIUM, https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47#_ftn1 (last accessed Oct. 23, 2025).

47. But most internet users are completely unaware that substantial information about their internet usage is being collected through tracking Pixels. The FTC warns that:

> Traditional controls such as blocking third party cookies may not entirely prevent pixels from collecting and sharing information. Additionally, many consumers may not realize that tracking pixels exist because they're invisibly embedded within web pages that users might interact with…Academic and public reporting teams have found that thousands of the most visited webpages have pixels and other methods that leak personal information to third parties.[29]

iii. The Pixels Installed on mySNHU Transmit Personally Identifiable Information to Google and TikTok.

48. Every website is hosted by a computer "server" that holds the website's contents.

49. To access a website, individuals use "web browsers." Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as a computer, tablet, or smartphone) accesses web content through a web browser (such as Google's Chrome, Mozilla's Firefox, Apple's Safari, or Microsoft's Edge).

50. Communications between a website server and web browser consist of Requests and Responses. Any given browsing session may consist of hundreds or even thousands of individual Requests and Responses. A web browser's Request essentially asks the website to provide certain information, such as the contents of a given webpage when the user clicks a link, and the Response from the website sends back the requested information – the web pages' images, words, buttons, and other features that the browser shows on the user's screen as they navigate the website.

[29] *Lurking Beneath the Surface, supra* note 27.

51. Additionally, on most websites, the Response sent back to the user's web browser directs the browser to create small files known as 'cookies' on the user's device.[30] These cookies are saved by the user's web browser, and are used to identify the website user as they browse the website or on subsequent visits to the site.[31] For example, in a more innocuous use case, a cookie may allow the website to remember a user's name and password, language settings, or shopping cart contents.[32]

52. When a Tracking Tool Provider accountholder logs onto their account, their web browser records a tracking cookie.[33] These cookies include a specific line of code that links the web browser to the user's account with the Tracking Tool Provider.[34]

53. The Google and TikTok Pixels use cookies, but operate differently than cookies. Rather than directing the browser to save a file on the user's device, the Pixels acquire information from the browser, without notifying the user. The information can include details about the user, his or her interactions with the website, and information about the user's environment (*e.g.,* type of device, type of browser, and sometimes even the physical location of the device).

54. Simultaneously, the Pixels, like those installed on mySNHU, request identifying information from any of the Tracking Tool Provider' cookies previously installed on the user's web browser.

55. The Pixel then combines the data it received from the browser with the data it acquired from the cookie, and instructs the web browser to transmit the information back to Google

---

[30] *What is a web browser?*, MOZILLA, https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/ (last accessed Oct. 23, 2025).

[31] *Id*.

[32] *Id*.

[33] Cyphers, *supra* note 11.

[34] *Id*.

and TikTok. As a result, Google and TikTok can link all of the user information collected by their Pixels on mySNHU to the user's identity, via the user's account or profile. Thus, even if a user never actually logs into a website, or fills out a form, the website, along with Google and TikTok, can know the user's identity.

56. A remarkable number of Americans possess a Google or TikTok account. One-third of Americans have accounts with Google's Gmail e-mail client, and over 80-percent of Americans use YouTube, Google's video client.[35] And, approximately one-third of Americans report using TikTok.[36] When these users visit a website, like mySNHU, that utilizes Google and TikTok's Tracking Tools, any information collected by the Pixels can be linked to the user's identity through the relevant cookies installed on the user's web browser.

57. However, it is not only accountholders of Google and TikTok that are at risk of having Pixel-collected website data linked to their identities. Rather, Google and TikTok utilize sophisticated data tracking methods to identify even those few users who do not have Google or TikTok accounts.

58. The Tracking Tools, like those on mySNHU, can acquire information about the user's device and browser, such as their screen resolution, time zone setting, browser software type and version, operating system type and version, language setting, and IP address.

---

[35] *See* Harsha Kiran, *49 Gmail Statistics To Show How Big It Is In 2024*, TECHJURY (Jan. 3, 2024), https://techjury.net/blog/gmail-statistics/ ((last accessed Oct. 23, 2025) ("Gmail accounts for 130.9 million of the total email users in the US"). The United States population is approximately 337.4 million. *See* UNITED STATES CENSUS BUREAU, https://www.census.gov/popclock/ (last accessed Oct. 23, 2025); Jeffrey Gottfried, *Americans' Social Media Use*, PEW RESEARCH (Jan. 31, 2024), https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/ (last visited Oct. 23, 2025).

[36] Jeffrey Gottfried, *Americans' Social Media Use*, PEW RESEARCH (Jan. 31, 2024), https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/ (last visited Oct. 23, 2025).

59. An internet user's combination of such device and browser characteristics, commonly referred to as their "browser fingerprint," is "often unique."[37] By tracking this browser fingerprint, Google and TikTok are able to compile a user's activity across the internet.[38] And, as Google and TikTok continuously compile user data over time, their understanding of the user's browser fingerprint becomes more sophisticated such that they need only to collect a single piece of identifying information to identify the user linked to a browser fingerprint.

iv. Defendant Disclosed Plaintiffs' and Class Members' Sensitive Information to Unauthorized Third Parties.

60. To attend SNHU, Plaintiffs and Class Members were required to use mySNHU, Defendant's online portal for students to manage their courses, access their academic records, and connect with faculty and other SNHU students.

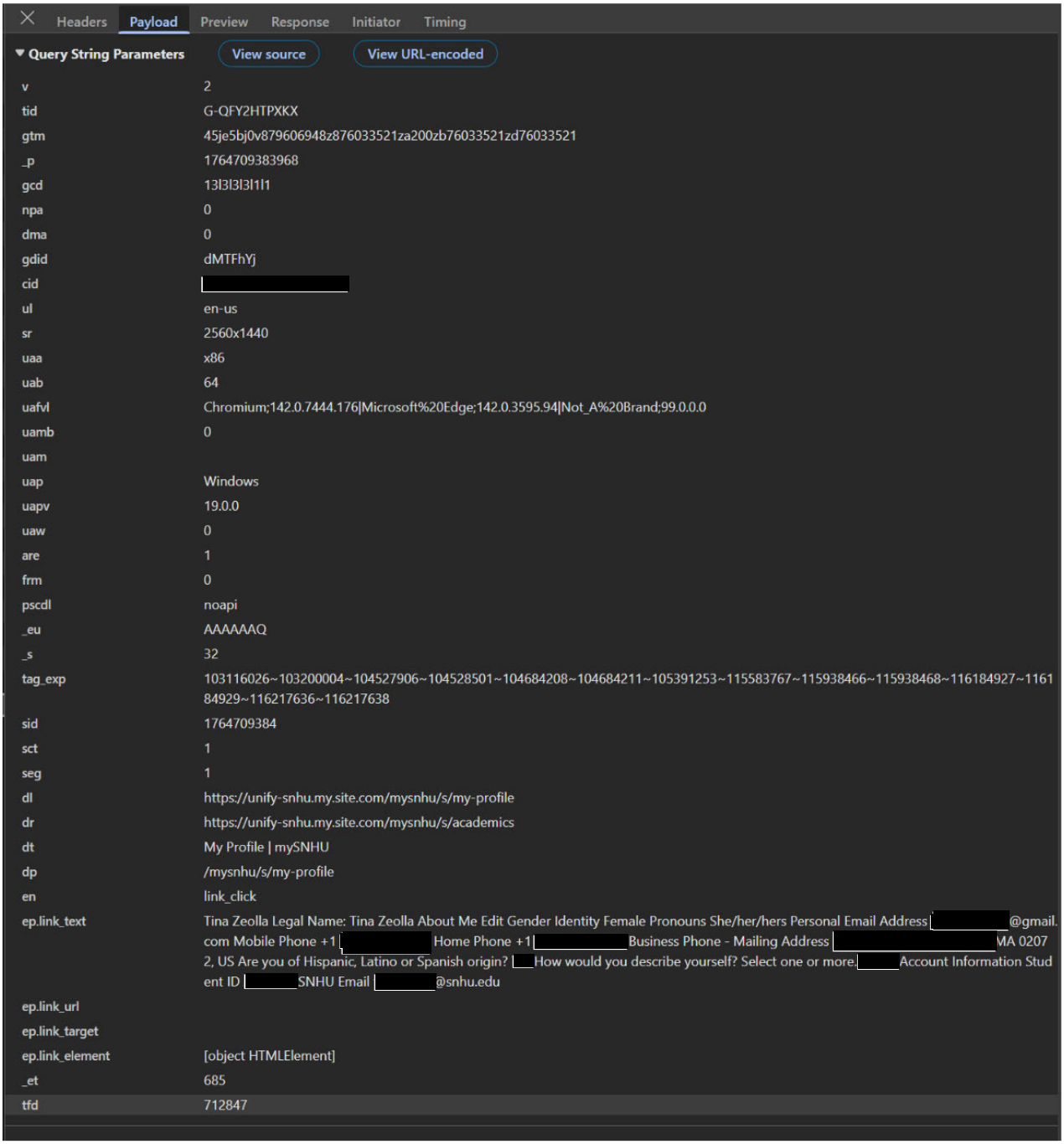
61. Unbeknownst to Plaintiffs and Class Members, Defendant intentionally configured the Tracking Tools installed on mySNHU to capture and transmit the Sensitive Information that they communicated to Defendant while using its student portal.

62. The following screenshots ("Figures 1-3") depict network transmissions made to Google by the Tracking Tools installed on mySNHU. As Figures 1-3 show, when SNHU students perform routine tasks in mySNHU, such as checking their course load or financial aid status, the information transmitted to Google by the Tracking Tools includes in plain English, the student's full name, e-mail address, phone number, address, ethnicity, gender identity, SNHU student ID number, career status, the fact that the student has or has not served in the military, the fact that the student is or is not a first-generation college student, the fact that the student has or has not applied

[37] Cyphers, *supra* note 11.

[38] *Id*.

for financial aid, detailed descriptions of every course in which the student is enrolled, and the student's cumulative GPA.[39]

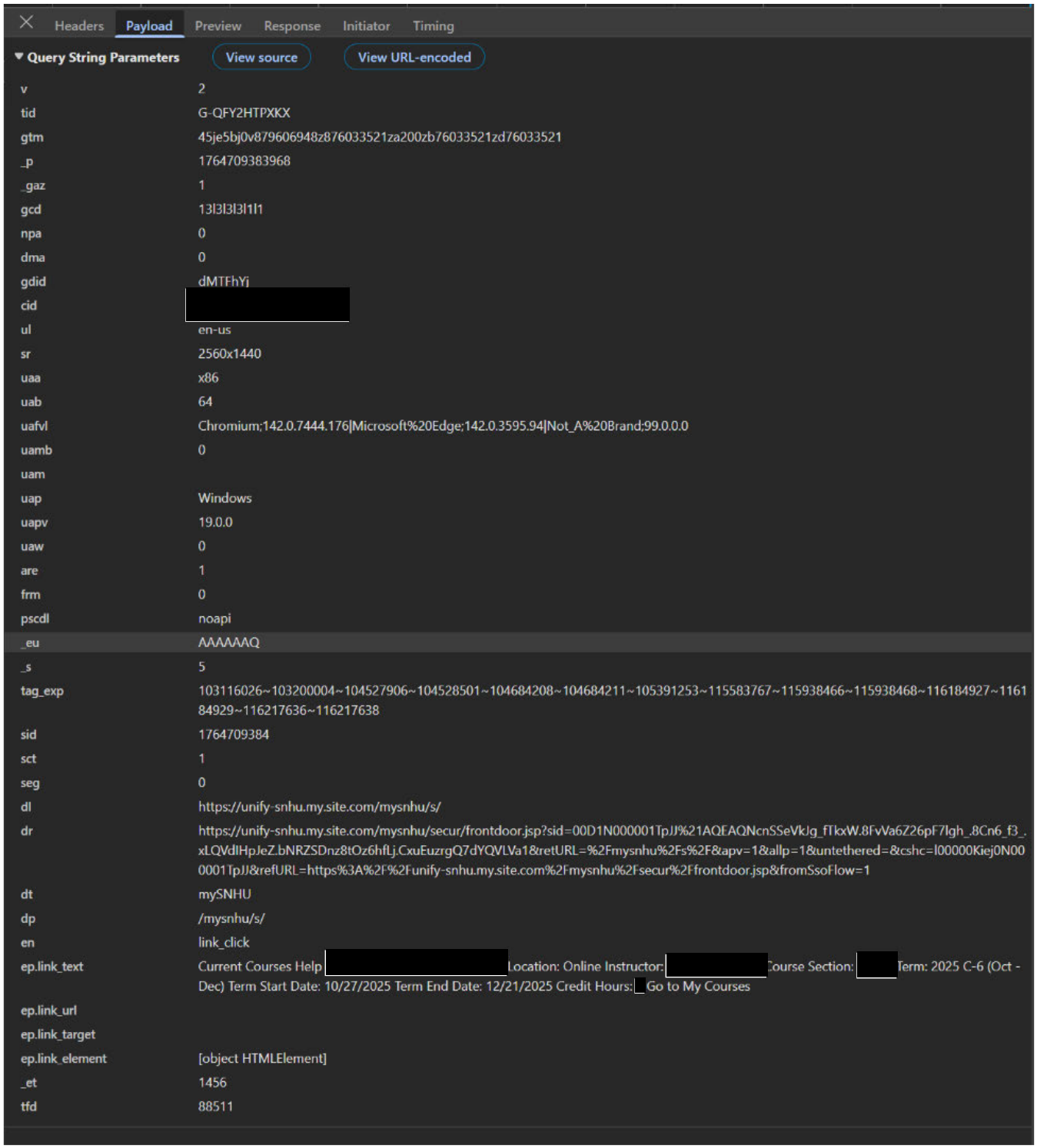


Headers | Payload | Preview | Response | Initiator | Timing

▼ Query String Parameters | View source | View URL-encoded

v	2
tid	G-QFY2HTPXKX
gtm	45je5bj0v879606948z876033521za200zb76033521zd76033521
_p	1764709383968
gcd	13l3l3l3l1l1
npa	0
dma	0
gdid	dMTFhYj
cid	[redacted]
ul	en-us
sr	2560x1440
uaa	x86
uab	64
uafvl	Chromium;142.0.7444.176|Microsoft%20Edge;142.0.3595.94|Not_A%20Brand;99.0.0.0
uamb	0
uam	
uap	Windows
uapv	19.0.0
uaw	0
are	1
frm	0
pscdl	noapi
_eu	AAAAAAQ
_s	32
tag_exp	103116026~103200004~104527906~104528501~104684208~104684211~105391253~115583767~115938466~115938468~116184927~116184929~116217636~116217638
sid	1764709384
sct	1
seg	1
dl	https://unify-snhu.my.site.com/mysnhu/s/my-profile
dr	https://unify-snhu.my.site.com/mysnhu/s/academics
dt	My Profile | mySNHU
dp	/mysnhu/s/my-profile
en	link_click
ep.link_text	Tina Zeolla Legal Name: Tina Zeolla About Me Edit Gender Identity Female Pronouns She/her/hers Personal Email Address [redacted]@gmail.com Mobile Phone +1 [redacted] Home Phone +1 [redacted] Business Phone - Mailing Address [redacted] MA 02072, US Are you of Hispanic, Latino or Spanish origin? [redacted] How would you describe yourself? Select one or more. [redacted] Account Information Student ID [redacted] SNHU Email [redacted]@snhu.edu
ep.link_url	
ep.link_target	
ep.link_element	[object HTMLElement]
_et	685
tfd	712847

[39] Figures 1-3 depict information collected from Plaintiff Tina Zeolla's mySNHU account. To protect the Plaintiff's privacy, her Sensitive Information has been redacted.



Headers | Payload | Preview | Response | Initiator | Timing

Query String Parameters View source View URL-encoded

v	2
tid	G-QFY2HTPXKX
gtm	45je5bj0v879606948z876033521za200zb76033521zd76033521
_p	1764709383968
_gaz	1
gcd	13l3l3l3l1l1
npa	0
dma	0
gdid	dMTFhYj
cid	[redacted]
ul	en-us
sr	2560x1440
uaa	x86
uab	64
uafvl	Chromium;142.0.7444.176|Microsoft%20Edge;142.0.3595.94|Not_A%20Brand;99.0.0.0
uamb	0
uam	
uap	Windows
uapv	19.0.0
uaw	0
are	1
frm	0
pscdl	noapi
_eu	AAAAAAQ
_s	5
tag_exp	103116026~103200004~104527906~104528501~104684208~104684211~105391253~115583767~115938466~115938468~116184927~116184929~116217636~116217638
sid	1764709384
sct	1
seg	0
dl	https://unify-snhu.my.site.com/mysnhu/s/
dr	https://unify-snhu.my.site.com/mysnhu/secur/frontdoor.jsp?sid=00D1N000001TpJJ%21AQEAQNcnSSeVkJg_fTkxW.8FvVa6Z26pF7lgh_.8Cn6_f3_.xLQVdlHpJeZ.bNRZSDnz8tOz6hfLj.CxuEuzrgQ7dYQVLVa1&retURL=%2Fmysnhu%2Fs%2F&apv=1&allp=1&untethered=&cshc=l00000Kiej0N000001TpJJ&refURL=https%3A%2F%2Funify-snhu.my.site.com%2Fmysnhu%2Fsecur%2Ffrontdoor.jsp&fromSsoFlow=1
dt	mySNHU
dp	/mysnhu/s/
en	link_click
ep.link_text	Current Courses Help [redacted] Location: Online Instructor: [redacted] Course Section: [redacted] Term: 2025 C-6 (Oct - Dec) Term Start Date: 10/27/2025 Term End Date: 12/21/2025 Credit Hours: Go to My Courses
ep.link_url	
ep.link_target	
ep.link_element	[object HTMLElement]
_et	1456
tfd	88511

Figures 1-3. Screenshots depicting back-end network traffic from mySNHU which shows information transmitted to Google when students use various mySNHU functions.

63. In addition to including Plaintiffs' full names, addresses, phone numbers, and e-mail addresses, the Sensitive Information that was transmitted to Google was additionally

accompanied by specific lines of code linking the Sensitive Information to Plaintiffs. As shown in Figures 1-3, the Google Tracking Tools on mySNHU transmitted the identifier numbers attached to Google's 'cid' and 'sid' cookies, which identify the user's Google account, as well as information commonly used to make a browser fingerprint, including the user's operating system and version, browser software and version, screen resolution, and language.

64. Defendant similarly tracks visitors to its publicly facing website, https://www.snhu.edu/ (the "SNHU Website") using Google Tracking Tools, as well as Tracking Tools developed by Facebook, Pinterest, and TikTok.

65. To illustrate, the following screenshot ("Figure 4") depicts network transmissions made to TikTok by the Tracking Tools installed on the SNHU Website. As Figure 4 shows, when visitors to the SNHU Website navigate the Website to obtain information regarding SNHU's academic programs, admission requirements, and tuition and financial aid options, browsing information, including detailed URL and site heading information, is transmitted to TikTok by the Tracking Tools, accompanied by identifier numbers attached to TikTok's (deceptively named) 'anonymous id' cookie, which identify the user's TikTok account.

/

/

/

/

/

/

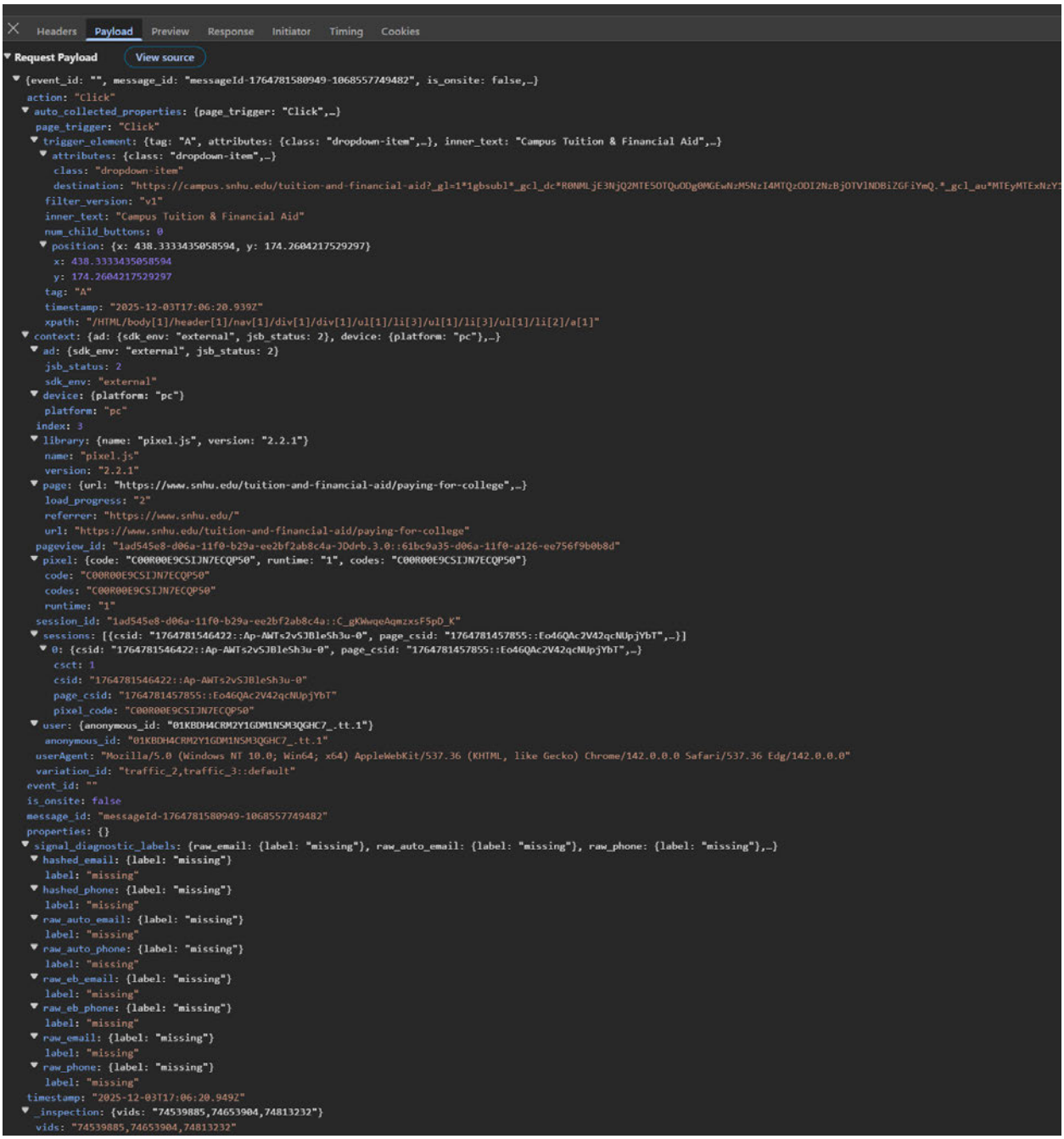


Figure 4. Screenshot depicting back-end network traffic from the SNHU Website which shows information transmitted to TikTok when students navigate the Website for information on tuition and financial aid.

66. When they are installed on a website, by default the Tracking Tools record and transmit only "automatic events," consisting largely of routine user behavior, such as clicking a link, clicking on an advertisement, or viewing a webpage. Defendant purposely configured the

Tracking Tools on mySNHU and the SNHU Website to collect and transmit additional user data, including the copious student record information depicted above.

B. DEFENDANT DISCLOSED PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES WITHOUT THEIR KNOWLEDGE OR CONSENT

i. Defendant failed to inform Plaintiffs and Class Members of its disclosure of Plaintiffs' and Class Members' Sensitive Information.

67. Defendant ***never*** informed Plaintiffs or Class Members that it was sharing their personally identifiable Sensitive Information with third parties, including Google and TikTok.

68. By engaging in this improper sharing of information without Plaintiffs' and Class Members' consent, Defendant breached Plaintiffs' and Class Members' right to privacy and unlawfully disclosed their Sensitive Information.

69. Despite never telling users like Plaintiffs and Class Members, Defendant allowed third parties such as Google and TikTok to intercept Plaintiffs' and Class Members' Sensitive Information and use it for advertising purposes.

ii. The Tracking Tools Used by Defendant Were Imperceptible to Plaintiffs and Class Members

70. The Tracking Tools installed on mySNHU were invisible to Plaintiffs and Class Members. Without analyzing the network information transmitted by mySNHU through examination of its source code or the use of sophisticated web developer tools, there was no way for a mySNHU user to discover the presence of the Tracking Tools. As a result, typical internet users, such as Plaintiffs and Class Members, were unable to detect the Tracking Tools on mySNHU.

71. Plaintiffs and Class Members were shown no disclaimer or warning that their Sensitive Information would be disclosed to any unauthorized third party without their express consent.

72. Plaintiffs and Class Members did not know that their Sensitive Information was being collected and transmitted to an unauthorized third party.

73. Because Plaintiffs and Class Members were not aware of the Tracking Tools on mySNHU, or that their Sensitive Information would be collected and transmitted to Google and TikTok, they could not and did not consent to Defendant's conduct.

C. DEFENDANT WAS ENRICHED BY THEIR DISCLOSURE OF PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION TO THIRD PARTIES

i. Defendant Received Material Benefits in Exchange for Plaintiffs' Sensitive Information

74. As explained, *supra*, users of the Business Tools, like Defendant, receive access to advertising and marketing analytics services in exchange for installing Google and TikTok's Tracking Tools on their website.

75. Upon information and belief, Defendant, as a user of Google and TikTok's Business Tools, received compensation in the form of advanced advertising services and cost-effective marketing on third-party platforms in exchange for allowing Google and TikTok to collect Plaintiffs' and Class Members' Sensitive Information.

ii. Plaintiffs' and Class Members' Data Had Financial Value

76. Moreover, Plaintiffs' and Class Members' Sensitive Information has value, and Defendant's disclosure and interception of that Sensitive Information harmed Plaintiffs and the Class.

77. According to Facebook, another major internet advertiser, the value it derives from user data has continuously risen. "In 2013, the average American's data was worth about $19 per

year in advertising sales to Facebook, according to its financial statements. In 2020, [it] was worth $164 per year."[40]

78. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

79. Several companies have products through which they pay consumers for a license to track certain information. Indeed, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies, in addition to Google, that pay for browsing history information.

80. The unauthorized disclosure of Plaintiffs' and Class Members' private and Sensitive Information has diminished the value of that information, resulting in harm including to Plaintiffs and Class Members.

D. DEFENDANT'S USE OF THE TRACKING TOOLS VIOLATES FERPA

i. FERPA protects the confidentiality of education records.

81. FERPA, 20 U.S.C. § 1232g, *et seq*. and its implementing regulations govern the release of and access to "education records." *See* 20 U.S.C. § 1232(g); 34 C.F.R. Part 99.

82. Under FERPA, "education records" are "those records, files, documents, and other materials which – (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution." 20 U.S.C. § 1232g(a)(4)(A). The term "student" includes "any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution." 20 U.S.C. §

[40] Geoffrey A. Fowler, *There's no escape from Facebook, even if you don't use it*, THE WASHINGTON POST (Aug. 29, 2021), https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/ (last visited Mar. 7, 2025).

1232(g)(a)(6). Education records "include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files."[41]

83. Under the regulations implementing FERPA, "personally identifiable information" includes, but is not limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address of the student or student's family; (d) a personal identifier, such as the student's social security number, student number, or biometric record; (e) other indirect identifiers such as the student's date of birth, place of birth, and mother's maiden name; (f) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in a school community who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and (g) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the educational record relates." 34 C.F.R. 99.3.

84. Under FERPA, an educational institution or agency may not disclose personally identifiable information from a student's education records without signed and dated written consent, subject to exceptions not applicable here. *See* 34 C.F.R. 99.30-31.

ii. Defendant's use of the Tracking Tools violated FERPA.

85. Plaintiffs and Class Members, as past or present students enrolled at SNHU, are students of SNHU under FERPA. *See* 20 U.S.C. § 1232(g)(a)(6).

86. The information disclosed to Google and TikTok through the Tracking Tools, which includes Plaintiffs' and Class Members' cumulative GPAs, course enrollment, and financial aid status, are inarguably education records regulated by FERPA.

[41] *What is an education record?*, UNITED STATES DEPARTMENT OF EDUCATION, https://studentprivacy.ed.gov/faq/what-education-record (last accessed Dec. 2, 2025).

87. Defendant's disclosure of these education records alongside Plaintiffs' and Class Members' full names, e-mail addresses, phone numbers, addresses, and Google and TikTok cookie identifiers, without obtaining Plaintiffs' and Class Members' consent, thus constitutes a violation of FERPA.

E. PLAINTIFFS' AND CLASS MEMBERS' REASONABLE EXPECTATION OF PRIVACY

88. At all times when Plaintiffs and Class Members provided their Sensitive Information to Defendant, they each had a reasonable expectation that the information would remain confidential and that Defendant would not share the Sensitive Information with third parties for a commercial purpose.

89. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative informed consent before an entity collects and shares that individual's data to be one of the most important privacy rights.

90. For example, a recent Consumer Reports study shows that 92-percent of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[42]

91. Moreover, students are particularly concerned about data privacy with regards to student records. Indeed, one study found that students are less comfortable with their university sharing their data than they are of even Amazon sharing their data.[43] In explaining this finding, the

[42] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907 (last visited Mar. 7, 2025).

[43] *See* Maina Korir, Sharon Slade, Wayne Holmes, Yingfei Héliot, Bart Rienties, *Investigating the dimensions of students' privacy concern in the collection, use and sharing of data for learning analytics*, COMPUTERS IN HUM. BEHAV. REP'TS (March 2023).

researchers posited that "it may be that many are already aware of data sharing in a commercial context, but less aware, and potentially therefore, more disturbed by, data sharing in an educational context."[44] This is especially true given that federal and state laws, like FERPA broadly protect student information, and thereby create an expectation of privacy by students.

92. Personal data privacy and obtaining consent to share Sensitive Information are material to Plaintiffs and Class Members.

V. TOLLING AND ESTOPPEL

93. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of the incorporation of the Tracking Tools onto mySNHU.

94. The Tracking Tools on mySNHU were and are invisible to the average website visitor.

95. Through no fault or lack of diligence, Plaintiffs and Class Members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

96. Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

97. Defendant had exclusive knowledge that mySNHU incorporated the Pixels and other Tracking Tools and yet failed to disclose to students, including Plaintiffs and Class Members, that by using mySNHU, Plaintiffs' and Class Members' Sensitive Information would be disclosed or released to unauthorized third parties, including Google and TikTok.

98. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its students' Sensitive Information. In fact, to the present, Defendant has not conceded, acknowledged, or otherwise

[44] *Id.*

indicated to their students that they have disclosed or released their Sensitive Information to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

99. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

100. The earliest that Plaintiffs or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of this Complaint.

VI. CLASS ALLEGATIONS

101. This action is brought by the named Plaintiffs on their behalf and on behalf of a proposed Class of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

102. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

The Nationwide Class

All present or former students of SNHU who used mySNHU, and whose Sensitive Information was disclosed or transmitted to Google, TikTok, or any other unauthorized third party.

103. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of separate Michigan and Massachusetts Subclasses, which are defined as follows:

Michigan Subclass

All present or former students of SNHU residing in Michigan who used mySNHU, and whose Sensitive Information was disclosed or transmitted to Google, TikTok, or any other unauthorized third party.

Massachusetts Subclass

All present or former students of SNHU residing in Massachusetts who used mySNHU, and whose Sensitive Information was disclosed or transmitted to Google, TikTok, or any other unauthorized third party.

104. Excluded from the proposed Class are any claims for personal injury, wrongful death, or other property damage sustained by the Class; Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns; and any Judge conducting any proceeding in this action and members of their immediate families.

105. Plaintiffs reserve the right to amend the definitions of the Class or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

106. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. On information and belief, there are at least 100,000 individuals that have been impacted by Defendant's actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendant.

107. **Commonality.** Common questions of law or fact arising from Defendant's conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class Members. These common questions include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the Sensitive Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Sensitive Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Sensitive Information would be disclosed to third parties;

d. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Sensitive Information was being disclosed without their consent;

e. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to keep the Sensitive Information belonging to Plaintiffs and Class Members free from unauthorized disclosure;

f. Whether Defendant violated the statutes asserted as claims in this Complaint;

g. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

h. Whether Defendant knowingly omitted material representations with respect to their data security and/or privacy policy practices; and

i. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their Sensitive Information.

108. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Sensitive Information, like that of every other Class Member, was compromised as a result of Defendant's incorporation and use of the Tracking Tools.

109. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

110. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was unlawfully stored and disclosed to unauthorized third parties, including Google and TikTok, in the same way.

The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

111. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

112. Defendant acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

113. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a) Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Sensitive Information and not disclosing it to unauthorized third parties;

b) Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;

c) Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d) Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Sensitive Information would be disclosed to third parties;

e) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties; and

f) Whether Class Members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendant's wrongful conduct.

114. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the unauthorized disclosures that have taken place.

COUNT I
COMMON LAW INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Massachusetts and Michigan Subclasses)

115. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 114 as if fully set forth herein.

116. Plaintiffs and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, highly personal Sensitive Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to the exfiltration of their communications without Plaintiffs' and Class Members' knowledge or consent.

117. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its website, including mySNHU and the communications platforms and services therein.

118. Plaintiffs and Class Members communicated Sensitive Information that they intended for only Defendant to receive and that they understood Defendant would keep private and secure.

119. Defendant's interception and disclosure of the substance and nature of those communications to third parties without the knowledge and informed consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

120. Plaintiffs and Class Members have a general expectation that their communications regarding sensitive, highly personal information would be protected from surreptitious disclosure to third parties.

121. Defendant's disclosure and publicization of Plaintiffs' and Class Members' Sensitive Information coupled with individually identifying information is highly offensive to the reasonable person.

122. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury including, but not limited to, an invasion of their privacy rights.

123. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to compensatory and/or nominal damages.

124. Plaintiffs and Class Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of the intrusions upon their privacy.

125. Plaintiffs and Class Members are also entitled to punitive damages resulting from

the malicious, willful and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

126. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT II
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Massachusetts and Michigan Subclasses)

127. Plaintiffs repeat and reallege the allegations contained in in paragraphs 1 through 126 as if fully set forth herein.

128. Through their enrollment as students of SNHU and use of mySNHU, Plaintiffs and Class Members provided Defendant with their Sensitive Information, believing such Information would be kept confidential.

129. By collecting and storing this data, Defendant had a duty of care to use reasonable means to secure and safeguard it from unauthorized disclosure to third parties.

130. Defendant negligently failed to take reasonable steps to protect Plaintiffs' and Class Members' Sensitive Information from being disclosed to third parties, without their consent, including to Google and TikTok.

131. Defendant further negligently omitted to inform Plaintiffs and the Class that they would use their Sensitive Information for marketing purposes, and/or that their Sensitive Information would be transmitted to third parties.

132. Defendant knew, or reasonably should have known, that Plaintiffs and the Class would not have provided their Sensitive Information to Defendant or used mySNHU had they known that Defendant intended to use that Information for unlawful purposes.

133. Defendant's conduct has caused Plaintiffs and the Class to suffer damages by

having their highly personal, personally identifiable Sensitive Information accessed, stored, and disseminated without their knowledge or consent.

134. Plaintiffs and Class Members are entitled to compensatory, nominal, and/or punitive damages.

135. Defendant's negligent conduct is ongoing, in that it still holds the Sensitive Information of Plaintiffs and Class Members in an unsafe and unsecure manner. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Massachusetts and Michigan Subclasses)

136. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 135 as if fully set forth herein.

137. When Plaintiffs and Class Members provided their Sensitive Information to Defendant in exchange for enrollment of courses and use of the mySNHU student portal, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose the Sensitive Information without consent.

138. Plaintiffs and Class Members accepted Defendant's offers and provided their Sensitive Information to Defendant.

139. Plaintiffs and Class Members would not have entrusted Defendant with their Sensitive Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Sensitive Information without consent.

140. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Sensitive Information to third parties like Google and TikTok.

141. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

142. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially less for those services, had they known their Sensitive Information would be disclosed.

143. Plaintiffs and Class Members are entitled to compensatory, consequential, and/or nominal damages as a result of Defendant's breaches of implied contract.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Massachusetts and Michigan Subclasses)

144. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 143 as if fully set forth herein.

145. Plaintiffs plead this claim in the alternative to their breach of implied contract claim.

146. Plaintiffs and Class Members conferred a monetary benefit on Defendant in exchange for educational services. Specifically, they provided their enrollment payments, as well as their Sensitive Information to Defendant which Defendant then utilized for marketing and advertising purposes, as described, *supra*.

147. Defendant knew that Plaintiffs and Class Members conferred a benefit upon them, which Defendant accepted. Defendant profited from the Sensitive Information of Plaintiffs and Class Members by exchanging it for marketing and advertising services.

148. In particular, Defendant enriched itself by obtaining the inherent value of Plaintiffs'

and Class Members' Sensitive Information, and by saving the costs it reasonably should have expended on marketing and/or data security measures to secure Plaintiffs' and Class Members' Sensitive Information.

149. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the privacy of its students' Sensitive Information.

150. Under the principles of equity and good conscience, Defendant should not be permitted to retain such benefits obtained by its surreptitious collection and transmission of Plaintiffs' and Class Members' Sensitive Information.

151. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Sensitive Information, they would not have agreed to provide their Sensitive Information to Defendant.

152. Plaintiffs and Class Members have no adequate remedy at law for this count. An unjust enrichment theory provides the equitable disgorgement of profits even where an individual has not suffered a corresponding loss in the form of direct money damages.

153. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury.

154. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them, or to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT V
VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA"), 18 U.S.C. § 2511(1), *et seq*.
Unauthorized Interception, Use, and Disclosure
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Massachusetts and Michigan Subclasses)

155. Plaintiffs repeat and reallege the allegations contained in the paragraphs 1 through 154 as if fully set forth herein.

156. The ECPA protects both sending and receipt of communications.

157. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

158. The transmissions of Plaintiffs' Sensitive Information to mySNHU qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

159. Electronic Communications. The transmission of Sensitive Information between Plaintiffs and Class Members and mySNHU with which they chose to exchange communications 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 photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

160. Content. The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

161. Interception. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or

other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

162. Electronical, Mechanical or Other Device. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Pixel code deployed by Defendant to effectuate the sending and acquisition of the Sensitive Information.

163. By utilizing and embedding the Pixels on mySNHU, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

164. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Pixels, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to third parties such as Google and TikTok.

165. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding their Sensitive Information, including extensive FERPA-protected information.

166. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to third parties, while knowing or having reason to know that such information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

167. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

168. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

169. The ECPA provides that a "party to the communication" may be liable where a "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." 18 U.S.C § 2511(2)(d).

170. Defendant is not a party to the communication based on its unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Sensitive Information does not qualify for the party exemption.

171. Defendant's acquisition of sensitive communications that were used and disclosed to Google and TikTok was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Invasion of privacy;

b. Breach of Implied Contract;

c. Violations of the New Hampshire Wiretap Act, N.H. Rev. Stat. § 570-A, *et seq.;* and

d. Violations of FERPA, 20 U.S.C. § 1232g, *et seq*.

172. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their Sensitive Information on mySNHU, because it used its participation in these communications to improperly share Plaintiffs' and Class Members' Private Information with Google and TikTok and other third-parties that (a) did not participate in these communications, (b) Plaintiffs and Class Members did not know were receiving their Sensitive Information, and (c) Plaintiffs and Class Members did not consent to receive their Sensitive Information.

173. As such, Defendant cannot viably claim any exception to ECPA liability.

174. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their Sensitive Information for commercial purposes has caused Plaintiffs and Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class Members' Sensitive Information without providing any value or benefit to Plaintiffs or Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' Sensitive Information, such as understanding how people use mySNHU and determining what ads people see on mySNHU, without providing any value or benefit to Plaintiffs or Class Members;

d. Defendant failed to provide Plaintiffs and Class Members with the full value of the services for which they paid, which included a duty to maintain the confidentiality of their Sensitive Information; and

e. The diminution in value of Plaintiffs' and Class Members' Sensitive Information and/or the loss of privacy due to Defendant making such Sensitive Information, which Plaintiffs and Class Members intended to remain private, no longer private.

175. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Tracking Tools to track and utilize Plaintiffs' and Class Members' Sensitive Information for financial gain.

176. Defendant was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

177. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy via the Pixels.

178. Any purported consent that Defendant may claim to have received from Plaintiffs and Class Members was not valid.

179. In sending and acquiring the content of Plaintiffs' and Class Members' communications relating to their use of mySNHU, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

180. As a result of Defendant's violation of the ECPA, Plaintiffs and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT VI
VIOLATIONS OF THE NEW HAMPSHIRE WIRETAP ACT
N.H. Rev. Stat. § 570-A, *et seq*.
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the Massachusetts and Michigan Subclasses)

181. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 180 as if fully set forth herein.

182. N.H. Rev. Stat. § 570-A:11 provides that "[a]ny person whose telecommunication or oral communication is intercepted, disclosed, or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose or use such communications[.]"

183. Telecommunication. The New Hampshire Wiretap Act defines "telecommunication" as "the transfer of any form of information in whole or in part through the facilities of a communications common carrier." N.H. Rev. Stat. § 570-A:1, I.

184. The transmissions of Plaintiffs' and Class Members' Sensitive Information to mySNHU falls within § 570-A:1's definition of "telecommunication."

185. Interception. The New Hampshire Wiretap Act defines "intercept" as "the aural or other acquisition of, or the recording of, the contents of any telecommunication or oral communication through the use of any electronic, mechanical, or other device." N.H. Rev. Stat. § 570-A:1, III.

186. Electronical, Mechanical or Other Device. The New Hampshire Wiretap Act defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a telecommunication or oral communication[.]" N.H. Rev. Stat. § 570-A:1, IV. The following constitute "devices" within the meaning of § 570-A:1, IV:

e. Plaintiffs' and Class Members' browsers;

f. Plaintiffs' and Class Members' computing devices;

g. Defendant's web-servers; and

h. The Pixel code deployed by Defendant to effectuate the sending and acquisition of the Sensitive Information.

187. Contents. The New Hampshire Wiretap Act defines "contents," when used with respect to telecommunications, to "include[] any information concerning the identity of the parties

to such communication or the existence, substance, purport, or meaning of that communication." N.H. Rev. Stat. § 570-A:1, VII.

188. By utilizing and embedding the Pixels on mySNHU, Defendant willfully intercepted, endeavored to intercept, and procured another person to intercept, the telecommunications of Plaintiffs and Class Members, in violation of N.H. Rev. Stat. § 570-A:2, I(a).

189. Specifically, Defendant intercepted Plaintiffs' and Class Members' telecommunications via the Pixels, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Sensitive Information to third parties such as Google and TikTok.

190. Defendant's intercepted telecommunications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding their Sensitive Information, including extensive FERPA-protected information.

191. By willfully disclosing or endeavoring to disclose the telecommunications of Plaintiffs and Class Members to third parties, while knowing or having reason to know that such information was obtained through the interception of a telecommunication in violation of N.H. Rev. Stat. § 570-A:2, (I)., Defendant violated N.H. Rev. Stat. § 570-A:2, I(c).

192. By willfully using, or endeavoring to use, the contents of the telecommunications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of a telecommunication in violation of N.H. Rev. Stat. § 570-A:2, (I)., Defendant violated N.H. Rev. Stat. § 570-A:2, I(d).

193. Defendant was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

194. Defendant did not obtain consent from Plaintiffs or Class Members prior to intercepting their telecommunications. *See* N.H. Rev. Stat. § 570-A:2, (I).

195. Further, any purported consent that Defendant may claim to have received from Plaintiffs and Class Members was not valid.

196. As a result of Defendant's violation of the New Hampshire Wiretap Act, Plaintiffs and Class Members are entitled to all damages available under N.H. Rev. Stat. § 570-A:11, including actual damages but not less than liquidated damages computed at a rate of $100 per day for each day of violation or $1,000, whichever is higher; punitive damages; reasonable attorney's fees and other reasonable litigation costs incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and other Class Members, pray for judgment against Defendant as follows:

A. an Order certifying the Nationwide Class, and Michigan and Massachusetts Subclasses, and appointing the Plaintiffs and their Counsel to represent the Classes;
B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Sensitive Information of Plaintiffs and Class Members;
C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;
D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;
E. an award of attorney fees, costs, and litigation expenses, as allowed by law;
F. prejudgment interest on all amounts awarded; and
G. all such other and further relief as this Court may deem just and proper.

Dated: December 17, 2025

Respectfully submitted,

/s/ Adam H. Weintraub
Adam H. Weintraub (# 275047)
WEINTRAUB LAW, LLC
170 Commerce Way, Suite 200
Portsmouth, New Hampshire 03801
Telephone: (603) 212-1785
Facsimile: (504) 708-4512
aweintraub@ahwfirm.com

Tyler J. Bean*
Sonjay C. Singh*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com
E: ssingh@sirillp.com

**pro hac vice admission anticipated*

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and other members of the proposed Classes, hereby demand a jury trial on all issues so triable.

Dated: December 17, 2025

Respectfully submitted,

/s/ Adam H. Weintraub
Adam H. Weintraub