GUTRIDE SAFIER LLP
Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie A. McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT FOR THE

NORTHERN DISTRICT OF CALIFORNIA

BARBARA MILES and JASON MANDLER, as individuals, on behalf of themselves, the general public, and those similarly situated, Plaintiffs, v. THE COCA-COLA COMPANY, Defendant.	CASE NO. CLASS ACTION COMPLAINT FOR INVASION OF PRIVACY; INTRUSION UPON SECLUSION; WIRETAPPING IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 631); COMMON LAW FRAUD, DECEIT AND/OR MISREPRESENTATION; AND UNJUST ENRICHMENT JURY TRIAL DEMANDED

TABLE OF CONTENTS

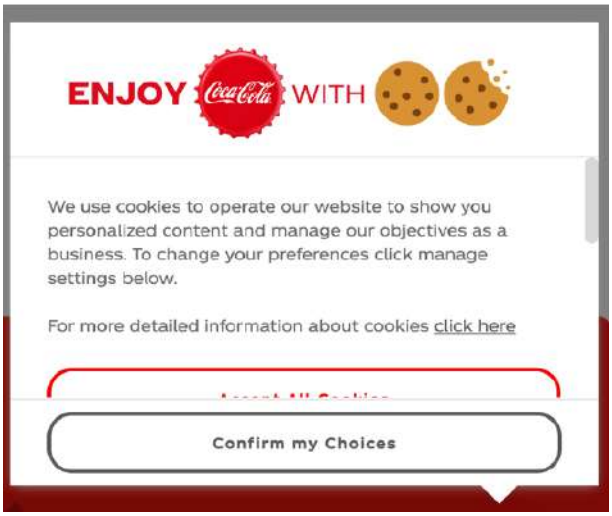
INTRODUCTION 1
THE PARTIES 4
FRAUDULENT CONCEALMENT AND TOLLING 4
JURISDICTION AND VENUE 5
SUBSTANTIVE ALLEGATIONS 5
A. Defendant Programmed the Websites to Include Third-Party Resources that Utilize Cookie-Based Tracking Technologies. 5
B. Defendant Falsely Informed Users That They Could Opt Out of, Decline, or Reject the Websites' Use of Cookies. 10
C. The Private Communications Intercepted and Collected Through Third-Party Cookies on Defendant's Websites. 33
1. Meta Cookies (Coca-Cola, Fairlife, BODYARMOR, Powerade, Fanta, Sprite, Vitaminwater, Simply, and Smartwater Websites). 33
2. Google Cookies (Coca-Cola, BODYARMOR, and Diet Coke Websites) 44
3. TikTok Cookies (Coca-Cola, Vitaminwater, Sprite, Fanta, and Smartwater Websites). 54
4. Microsoft Clarity Cookies (the Fairlife Website). 66
5. Snapchat Cookies (Coca-Cola, Fanta, Sprite, Powerade, Diet Coke, Vitaminwater, Fairlife, Simply, and Smartwater Websites). 68
6. Additional Third-Party Cookies 69
D. The Third Parties Intercept User Communications While in Transit. 73
E. The Private Communications Collected are Valuable. 78
PLAINTIFFS' EXPERIENCES 79
CLASS ALLEGATIONS 85
CAUSES OF ACTION 88
First Cause of Action: Invasion of Privacy 88
Second Cause of Action: Intrusion Upon Seclusion 90
Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631) 92
Fourth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation 96
Fifth Cause of Action: Unjust Enrichment 99
PRAYER FOR RELIEF 101

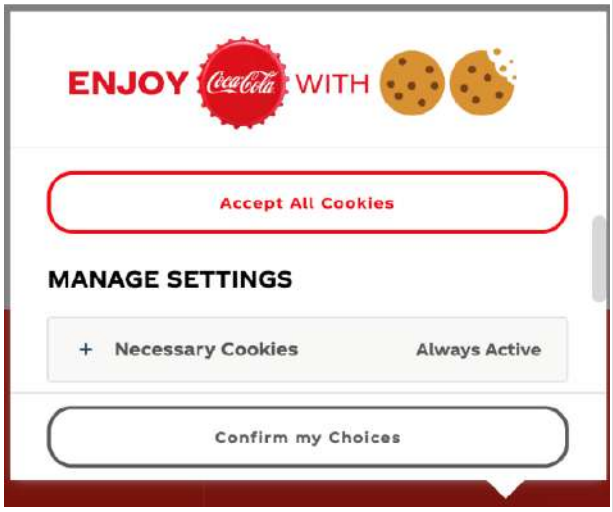
Plaintiff Barbara Miles and Plaintiff Jason Mandler (collectively, "Plaintiffs") bring this action on behalf of themselves, the general public, and all others similarly situated against The Coca-Cola Company ("Defendant" or "Coca-Cola"). Plaintiffs' allegations against Defendant are based on information and belief and the investigation of Plaintiffs' counsel, except for allegations specifically pertaining to Plaintiffs, which are based on their personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns egregious violations of consumer privacy and a breach of consumer trust in violation of California law. When consumers visit Defendant's websites (namely, coca-cola.com and us.coca-cola.com (collectively, the "Coca-Cola Website"), fanta.com (the "Fanta Website"), sprite.com (the "Sprite Website"), powerade.com (the "Powerade Website"), dietcoke.com (the "Diet Coke Website"), goldpeakbeverages.com (the "Gold Peak Website"), topochico.com (the "Topo Chico Website"), vitaminwater.com (the "Vitaminwater Website"), fairlife.com (the "Fairlife Website"), drinksimplybeverages.com (the "Simply Website"), drinkbodyarmor.com (the "BODYARMOR Website"), and drinksmartwater.com (the "Smartwater Website"); each a "Website" and collectively referred to as the "Websites"), Defendant displays to them a popup cookie consent banner. Defendant's cookie banner discloses that each Website uses cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendant assures visitors that they can choose to adjust the available toggle switches to decline, reject, or opt out of all categories of cookies in use on the Websites, including all categories of "Advertising," "Analytics," and (on some of the Websites) "Personalization" cookies, except those cookies "Necessary" for the Websites to function, as shown in the following example screenshots from the Coca-Cola Website:[1]

[1] At some point after January 2024, Defendant modified its cookie consent banner and/or cookie consent management platform on the Websites. Although the modified cookie consent banner continues to represent to Website visitors that they can reject, "turn off," or opt out of certain categories of cookies and tracking technologies, Defendant continues to cause Third Parties to intercept and collect Website users' Private Communications, including after users exercise their purported right to reject, "turn off," or opt out of such cookies and tracking technologies. Thus, notwithstanding Defendant's modifications to its cookie consent banner and/or cookie consent management platform, Defendant continues to disregard Website users'







2. Like most internet websites, Defendant designed the Websites to include resources and programming scripts from third parties that cause those parties to place cookies and other similar tracking technologies on visitors' browsers and devices and/or transmit cookies along with user data. Unlike many websites, however, Defendant affirmatively represented that users could browse the Websites without being tracked, followed, or targeted by third-party data brokers and advertisers. Those representations were false.

3. Even after users elect to decline or reject all categories of cookies in use on the Websites, including all categories of Advertising, Analytics, and Personalization cookies, except those cookies "Necessary" for the Websites to function, Defendant surreptitiously causes several third parties—including Meta Platforms, Inc. (Facebook), Google LLC (DoubleClick and

---

express privacy choices and permit the unauthorized interception and collection of their Private Communications by Third Parties.

Google Analytics), TikTok USDS Joint Venture LLC (TikTok), Microsoft Corporation (Microsoft Clarity), The Trade Desk, Inc. (adsrvr.org), Snap Inc. (Snapchat, tr.snapchat.com), Pinterest, Inc. (Pinterest), X Corp. (Twitter), and PubMatic, Inc.—to place and/or transmit cookies that track users' website browsing activities and intercept their private communications on the Websites (the "Third Parties").

4. Contrary to users' express declination or rejection of cookies and tracking technologies on the Websites, Defendant causes cookies, including the Third Parties' cookies, to be sent to Plaintiffs' and other visitors' browsers, stored on their devices, and intercepted by the Third Parties along with user data. These cookies permitted the Third Parties to track and collect data in real time regarding visitors' behaviors and communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is located in California.

5. The Third Parties analyze and aggregate this user data across websites and time for their own purposes and financial gain, including creating consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; creating audience segments based on shared traits (such as Millennials, Californians, tech enthusiasts, etc.); and performing targeted advertising and marketing analytics. Further, the Third Parties share user data and/or user profiles with unknown parties to further their financial gain.

6. This type of tracking and data sharing is exactly what the Websites' visitors sought to avoid when they adjusted settings to opt out of, decline, or reject all categories of Advertising, Analytics, and Personalization cookies on the Websites' cookie consent banner. Defendant falsely told the Websites' users that that they could decline, reject, or opt out of. Despite receiving clear notice of users' lack of consent, Defendant ignored those choices and violated state statutes and tort duties owed to Plaintiffs and those similarly situated users of the Websites.

THE PARTIES

7. Plaintiff Barbara Miles is, and was at all relevant times, an individual and resident of American Canyon, California. Plaintiff Miles intends to remain in California and makes her permanent home there.

8. Plaintiff Jason Mandler is, and was at all relevant times, an individual and resident of El Segundo, California. Plaintiff Mandler intends to remain in California and makes his permanent home there.

9. Defendant The Coca-Cola Company is a Delaware corporation with its headquarters and principal place of business in Atlanta, Georgia.

FRAUDULENT CONCEALMENT AND TOLLING

10. The delayed discovery rule applies to Plaintiffs' and Class members' claims. Plaintiffs and Class members were unaware that, despite rejecting all unnecessary cookies on the Websites, Defendant nonetheless caused third-party cookies to be sent to their browsers, stored on their devices, and intercepted by the Third Parties along with their private user data. Plaintiffs and Class members could not reasonably have discovered this conduct at the time of their visits to the Websites because it occurred through hidden, technical processes not visible to ordinary users. Nothing about Plaintiffs' or Class members' experiences on the Websites would have alerted a reasonable user that their selections were not being honored. Plaintiffs and Class members lacked the technical expertise and specialized tools necessary to determine whether the Websites honored their opt-out selections or instead continued transmitting their data notwithstanding their selections, and they did not discover Defendant's conduct until a later investigation revealed it.

11. Although they exercised reasonable diligence, Plaintiffs and Class members were unaware of Defendant's conduct because Defendant affirmatively represented that users could reject unnecessary cookies and tracking technologies, while simultaneously concealing that such tracking would occur regardless of users' selections. This combination of misrepresentation and omission prevented Plaintiffs and Class members from discovering their claims earlier. These

circumstances, including Defendant's concealment and misleading representations, warrant tolling the statute of limitations.

JURISDICTION AND VENUE

12. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2). The aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class consists of at least 100 members; and Plaintiffs and Defendant are citizens of different states.

13. The injuries, damages and/or harm upon which this action is based occurred or arose out of activities engaged in by Defendant within, affecting, and emanating from, the State of California. Defendant regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and services provided to persons in the State of California. Defendant has engaged, and continues to engage, in substantial and continuous business practices in the State of California.

14. Further, the Private Communications (defined below) and data that Defendant causes to be intercepted by the Third Parties are routed through servers located in California.

15. Venue is proper in this District 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 the State of California, including within this District.

16. A substantial part of the events or omissions giving rise to the claims in this action occurred in Napa County, California. Pursuant to Civil Local Rule 3-2(c) and (d), this action is properly assigned to the San Francisco/Oakland Division.

17. Plaintiffs accordingly allege that jurisdiction and venue are proper in this Court.

SUBSTANTIVE ALLEGATIONS

A. Defendant Programmed the Websites to Include Third-Party Resources that Utilize Cookie-Based Tracking Technologies.

18. Every website, including each of the Websites, is hosted by a server that sends and receives communications in the form of HTTP requests, such as "GET" or "POST" requests, to and from internet users' browsers. For example, when a user clicks on a hyperlink on any of

the Websites, the user's browser sends a "GET" request to that Website's server. The GET request tells the Website's server what information is being requested (e.g., the URL of the webpage being requested) and instructs the Website's server to send the information back to the user (e.g., the content of the webpage being requested). When the Website's server receives an HTTP request, it processes that request and sends back an HTTP response. The HTTP request includes the client's IP address, which allows the Website's server to identify the origin of the request and return the response.

19. An IP address (Internet Protocol address) is a unique numerical label assigned to each device connected to a network that uses the Internet Protocol for communication, typically expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4 addresses). IP addresses can identify the network a device is on and the specific device within that network. Public IP addresses used for internet-facing devices reveal geographical locations, such as country, city, or region, through IP geolocation databases.

20. As a result, Defendant knew or should have known that the devices used by Plaintiffs and Class members to access the Websites were located in California.

21. Defendant voluntarily integrated "third-party resources" from the Third Parties into its Websites' programming. "Third-party resources" refer to tools, content or services provided by third parties, such as analytics tools, advertising networks, or payment processors, that a website developer utilizes by embedding scripts, styles, media, or an application programming interface (API) into the website's code. Defendant's uses the third-party resources on the Websites pursuant to agreements between Defendant and the Third Parties.

22. The Websites cause users' devices to store and/or transmit both first-party and third-party tracking cookies. Cookies are small text files sent by a website server to a user's web browser and stored locally on the user's device. As described below, cookies generally contain a unique identifier which enables the website to recognize and differentiate individual users. Cookie files are sent back to the website server along with HTTP requests, enabling the website to identify the device making the requests, and to record a session showing how the user interacts with the website.

23. First-party cookies are those that are placed on the user's device directly by the web server with which the user is knowingly communicating (in this case, a Website's server). First-party cookies are used to track users when they repeatedly visit the same website.

24. A third-party cookie is set by a third-party domain/webserver (e.g., www.facebook.com, www.google.com, analytics.tiktok.com, etc.). When the user's browser loads a webpage (such as a webpage of any of the Websites) containing embedded third-party resources, the third parties' programming scripts typically issue HTTP commands to determine whether the third-party cookies are already stored on the user's device and to cause the user's browser to store those cookies on the device if they do not yet exist. Third-party cookies include an identifier that allows the third party to recognize and differentiate individual users across websites (including the Websites) and across multiple browsing sessions.

25. As described further below, the third-party cookies stored on and/or loaded from users' devices when they interact with the Websites are intercepted by those third parties, enabling them to surreptitiously track in real time and collect the Websites' users' personal information, such as their browsing activities and private communications with Defendant, including the following:

- **Browsing History**: Information about the webpages a Website's user visits, including the URLs, titles, and keywords associated with the webpages viewed, time spent on each page, and navigation patterns;
- **Visit History**: Information about the frequency and total number of visits to the Websites;
- **Website Interactions:** Data on which links, buttons, or ads on the Websites a user clicks;
- **User Input Data**: The information the user entered into a Website's form fields, including search queries, the user's name, age, gender, email address, location, and/or payment information;
- **Demographic Information**: Inferences about age, gender, and location based on browsing habits and interactions with the Websites' content;

- **Interests and Preferences**: Insights into user interests based on the types of content viewed, products searched for, or topics engaged with on the Websites;
- **Shopping Behaviors**: Information about the Websites' products viewed or added to shopping carts;
- **Device Information**: Details about a Website user's device, such as the type of device (mobile, tablet, desktop), operating system, and browser type;
- **Referring URL**: Information about the website that referred the user to the Websites;
- **Session Information**: Details about the user's current browsing session, including the exact date and time of the user's session, the session duration and actions taken on the Websites during that session;
- **User Identifiers**: A unique ID that is used to recognize and track a specific user of the Websites across different websites over time; and/or
- **Geolocation Data**: General location information based on the Website user's IP address or GPS data, if accessible, including whether the user is located in California.

(Collectively, the browsing activities and private communications listed in the bullet points above shall be referred to herein as "Private Communications.")

26. Third-party cookies can be used for a variety of purposes, including (i) analytics (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing campaigns); (ii) personalization (e.g., remembering a user's browsing history and purchase preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering targeted advertisements based on an aggregated profile of the user's behavior, preferences, and demographics); and (iv) social media integration (e.g., enabling sharing of users' activities with social media platforms). Ultimately, third-party cookies are utilized to enhance website performance and generate revenue through data collection and targeted advertising.

27. Defendant manufactures, markets, distributes, and sells a wide variety of nonalcoholic beverages under numerous brands, including Coca-Cola, Fanta, Sprite, Powerade,

Diet Coke, Gold Peak, Topo Chico, Vitaminwater, Fairlife, Simply, BODYARMOR, and Smartwater. Defendant maintains separate Websites associated with each of these brands, which allow visitors to, among other things, obtain information regarding Defendant's beverages and other products; browse and search for products; review product descriptions, ingredients and nutritional information; learn about particular brands, flavors, and product offerings; locate products and nearby retailers; access promotions, rewards, and other brand-related content; and, on certain Websites, purchase products, create or manage accounts, sign up for offers or other communications, and use other interactive features.

28. As users interact with the Websites—including by entering information into search fields and forms, searching for particular beverages, products, or other information, browsing product categories and individual products, reviewing product descriptions, ingredients, and nutritional information, searching for nearby retailers or product availability, accessing promotions and other brand content, clicking links, and making other selections—they communicate Private Communications to Defendant, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is located in California.

29. Defendant chose to install or integrate its Websites with resources from the Third Parties that, among other things, use cookies. Thus, when consumers visit the Websites, both first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is caused by software code that Defendant incorporates into its Websites, or that Defendant causes to be loaded. Because Defendant controls the software code of its Websites, and is capable of determining whether a user is accessing the Websites from California, it has complete control over whether first-party and third-party cookies are placed on its California users' devices and/or intercepted by third parties.

30. Defendant explained the third-party cookies it used on the Websites as follows in its Cookies Policy:

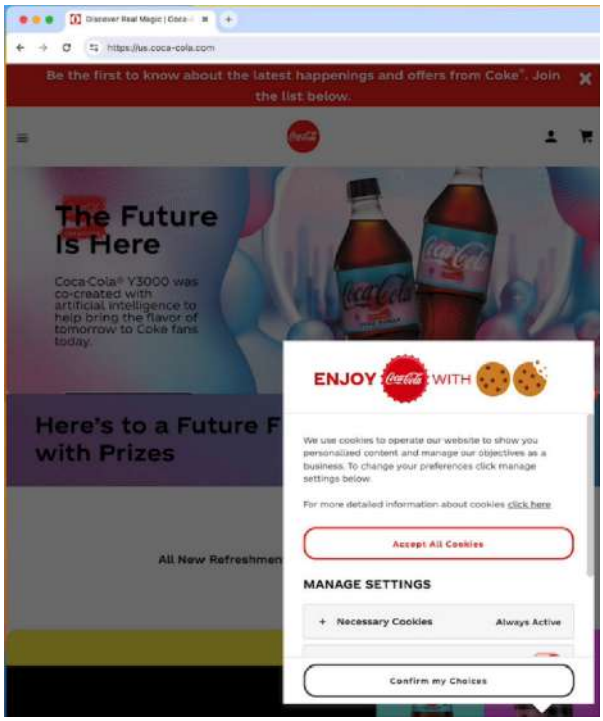
> Cookies are small pieces of text. They are provided by most websites and stored by your web browser on the computer, phone, or other device that you are using.

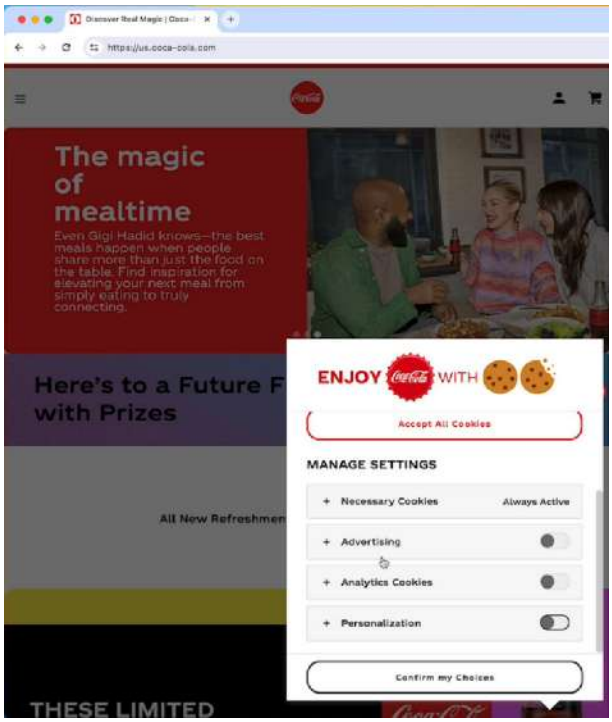
> Cookies serve many purposes. They can help a website remember your preferences, learn which areas of the website are useful and which areas need improvement, and provide you with targeted advertisements or personalized content. Sometimes, cookies are enabled when pixels are placed on a website. Pixels are also referred to as web beacons, clear gifs, and tags. They enable websites to read and place cookies.
>
> …
>
> A third-party cookie is one that you have received from another party, such as Google or Facebook. We do not control what third parties do on other sites. However, we may work with certain third-party providers such as Google or Facebook to permit their cookies to function through our Site so we can learn more about your web experience on our Site and better personalize our services for you.[2]

B. Defendant Falsely Informed Users That They Could Opt Out of, Decline, or Reject the Websites' Use of Cookies.

31. When Plaintiffs and other consumers in California visited any of the Websites, each Website immediately displayed to them a popup cookie consent banner, which was substantially similar on all of the Websites. As shown in the screenshot below, from the Coca-Cola Website, the cookie consent banner stated, "We use cookies to operate our website to show you personalized content and manage our objectives as a business. To change your preferences click manage settings below." The banner then purported to provide users the opportunity to "Accept All Cookies" but indicated that, rather than accepting all cookies, users could instead "Manage Settings" to decline, reject, or otherwise opt-out of all categories of cookies, including all "Advertising" cookies, "Analytics" cookies, and "Personalization" cookies, except the "Necessary Cookies" that are "Always Active," as shown in the following example screenshot from the Coca-Cola Website:

[2] The Coca-Cola Website Cookies Policy (updated October 2021) (available at https://www.coca-cola.com/us/en/legal/cookies-policy) (the "Cookies Policy"). Defendant has subsequently updated its Cookies Policy but, on information and belief, this version was in effect at the time of Plaintiffs' rejections of cookies on the Websites. On further information and belief, each of Defendant's Websites directed users to the same Cookies Policy.

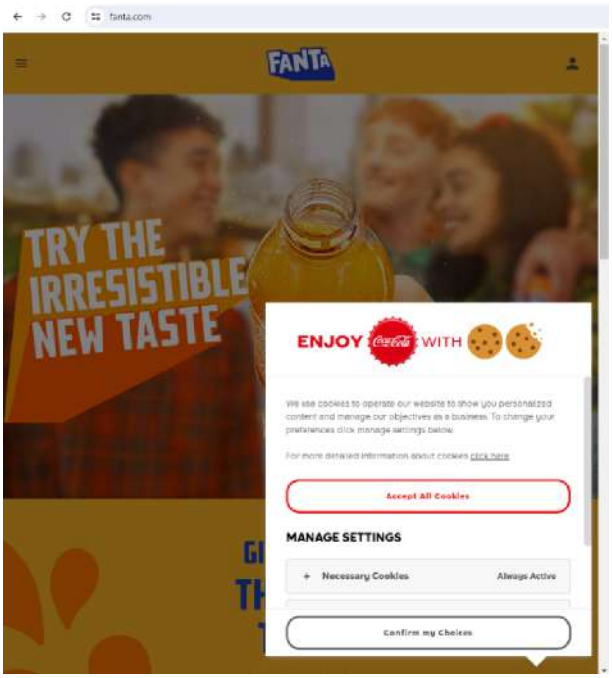


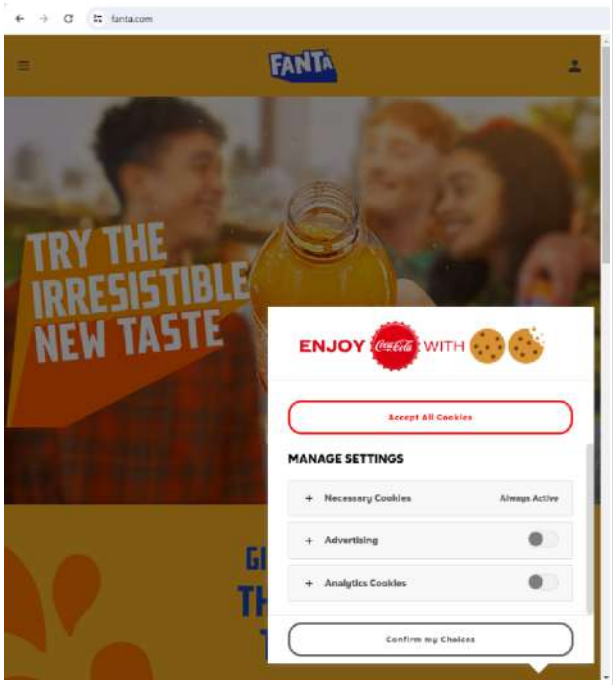


32. Each of the Websites made substantially similar representations. As shown in the screenshots below, each Website used the same scheme of prominently displaying a popup cookie consent banner claiming that users can "Manage Settings" for cookies to decline, reject, or opt out of all cookies used for or associated with "Advertising," "Analytics," and "Personalization":

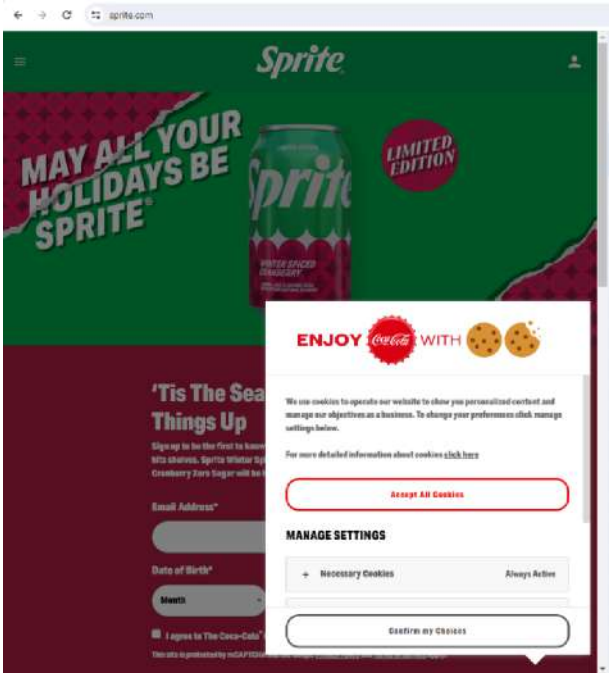
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

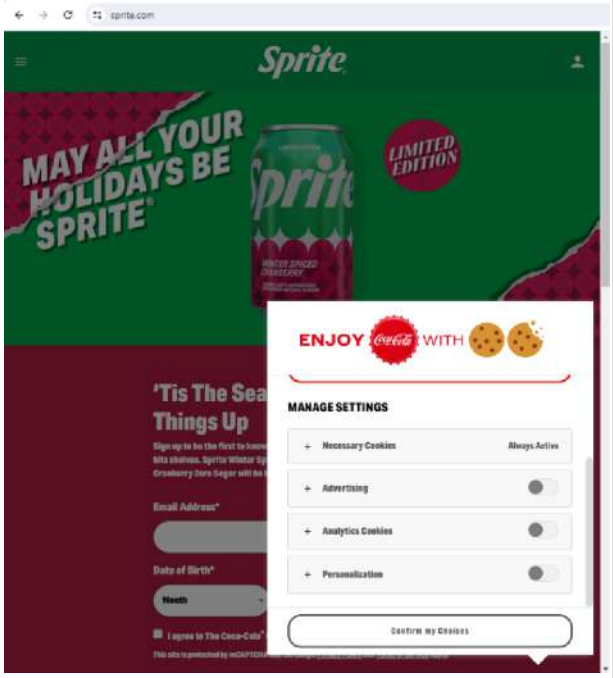
a. From the Fanta Website:



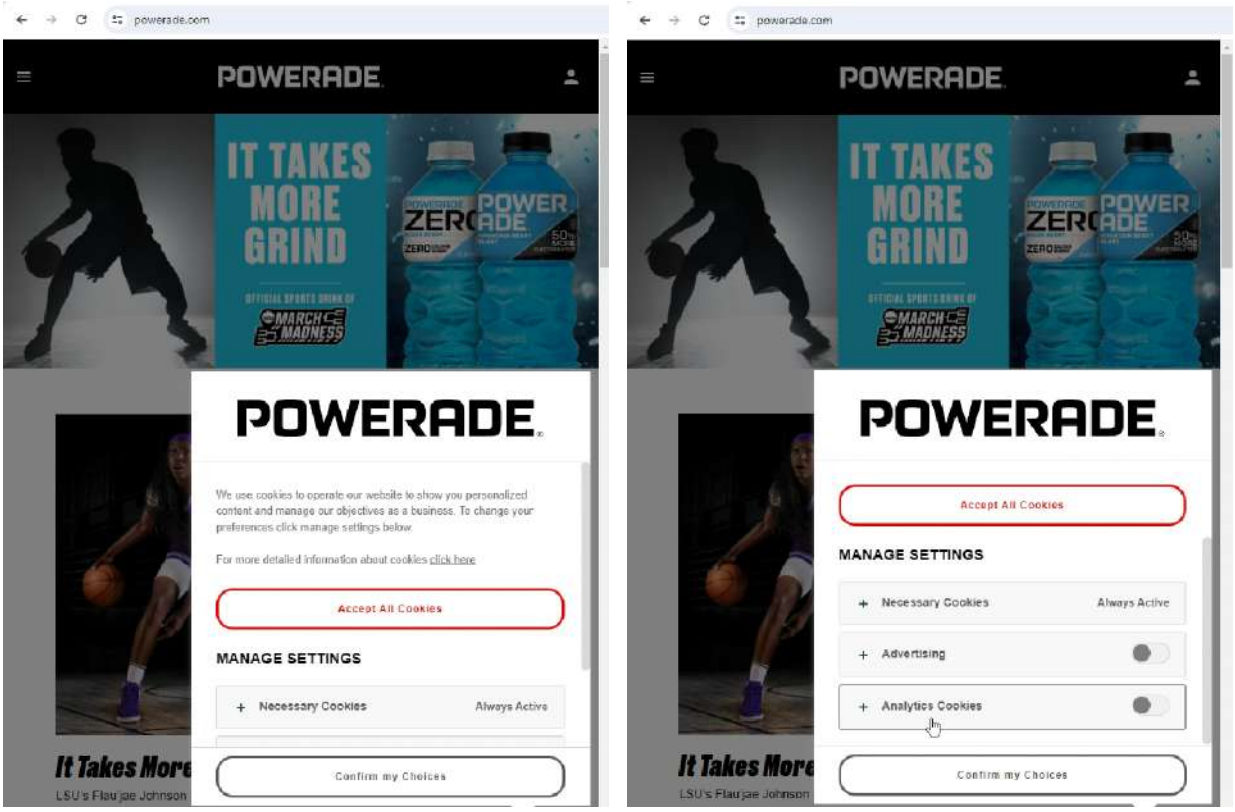


b. From the Sprite Website:

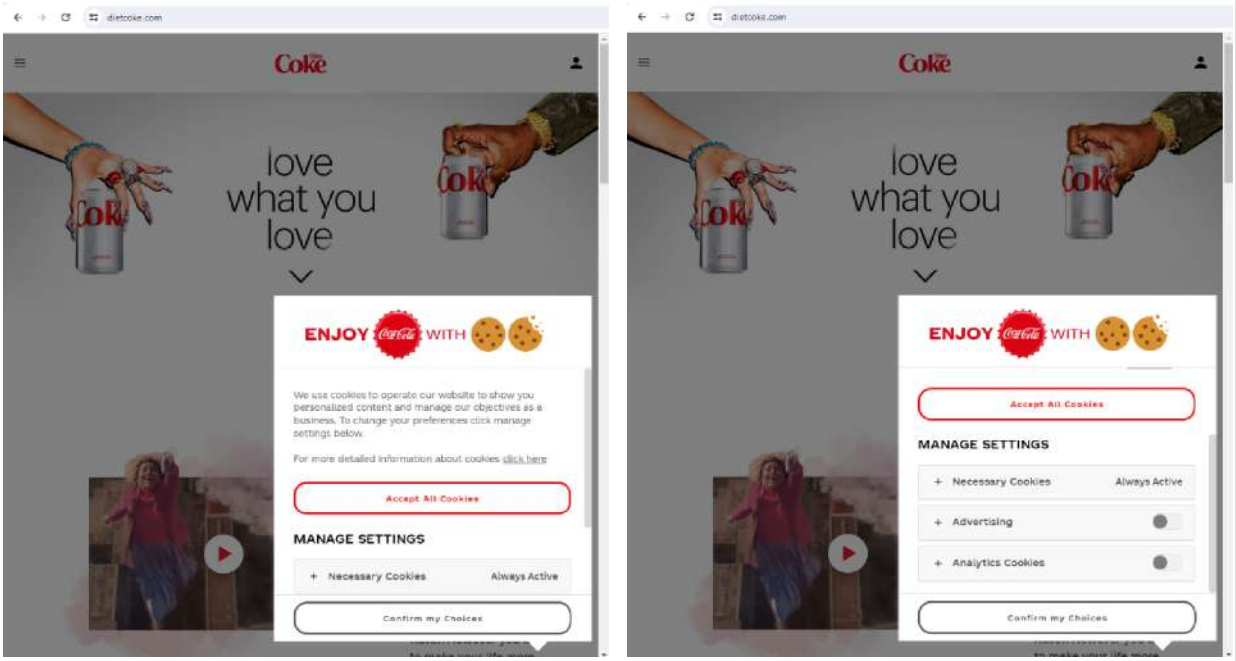




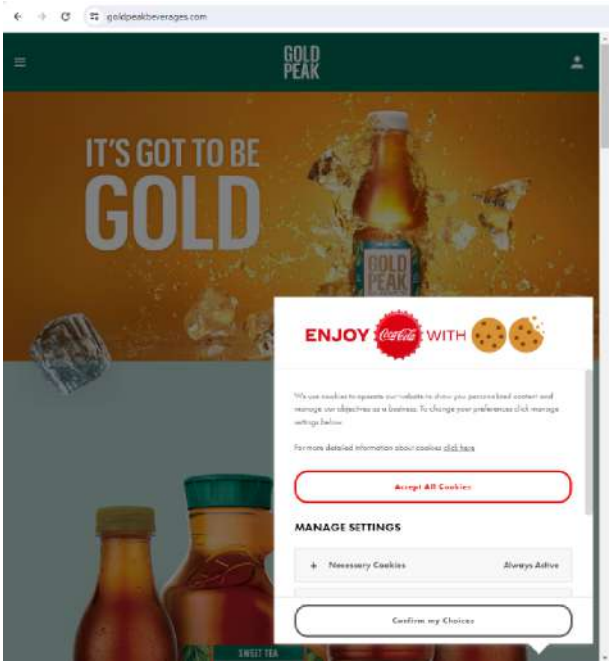
c. From the Powerade Website:

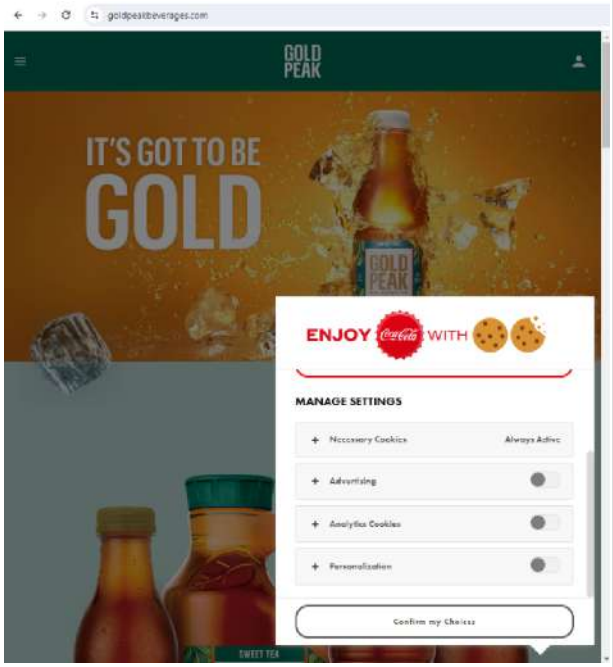


d. From the Diet Coke Website:

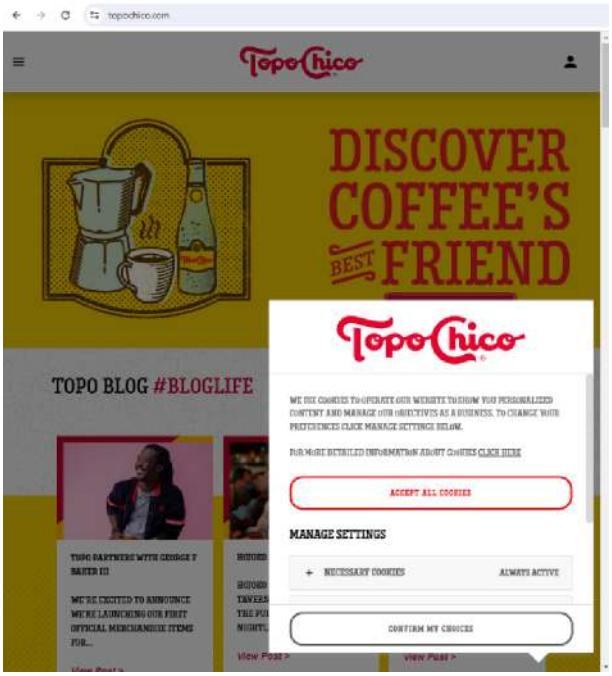


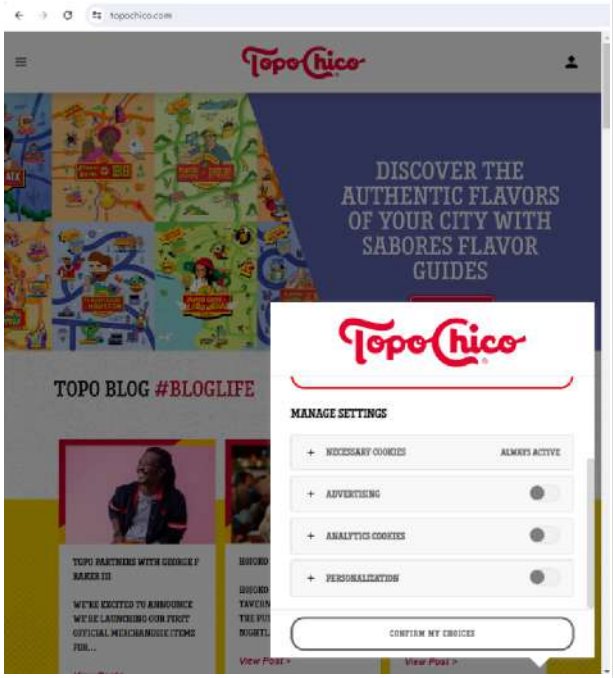
e. From the Gold Peak Website:



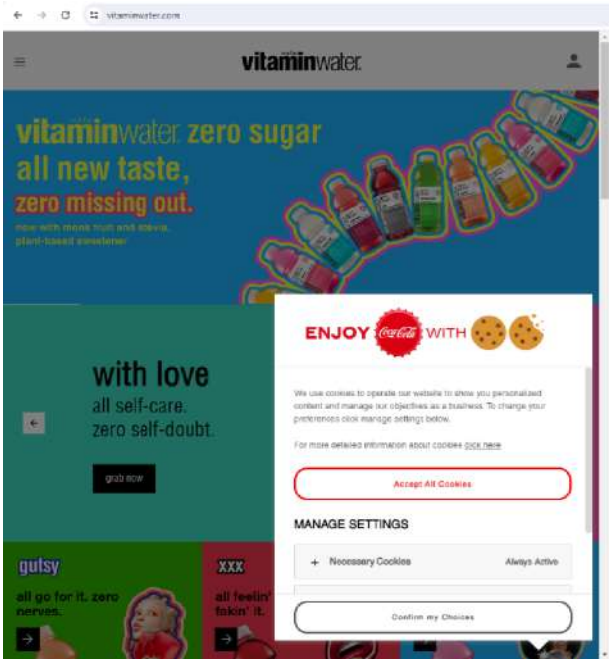


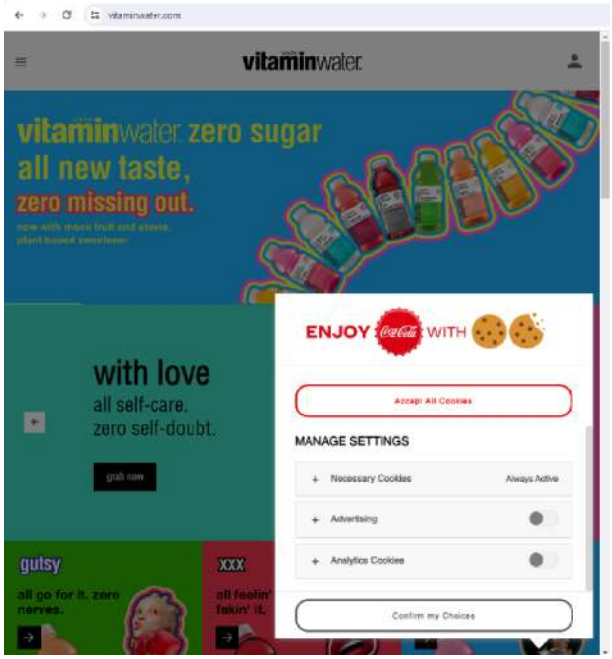
f. From the Topo Chico Website:



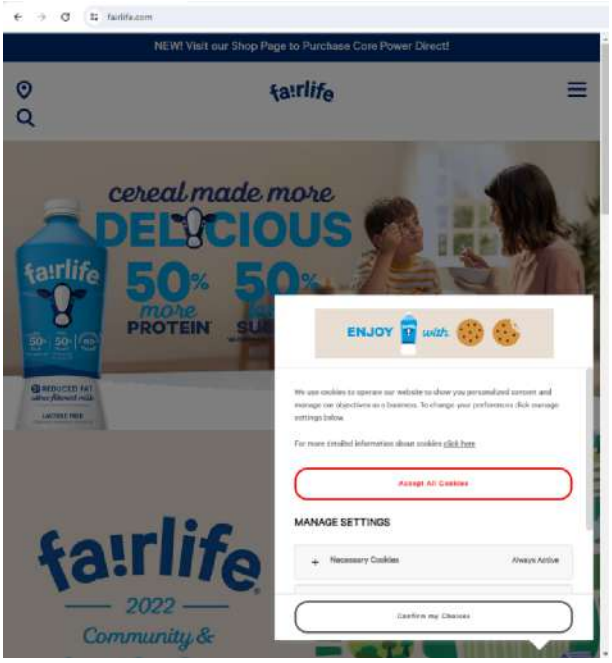


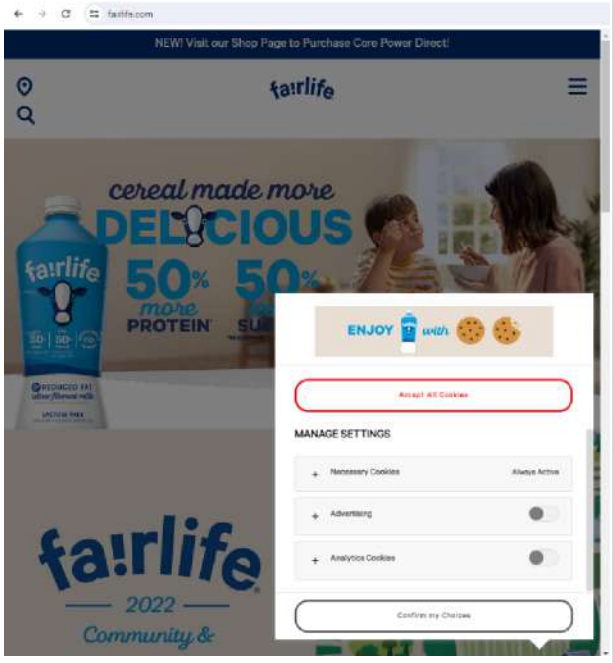
g. From the Vitaminwater Website:



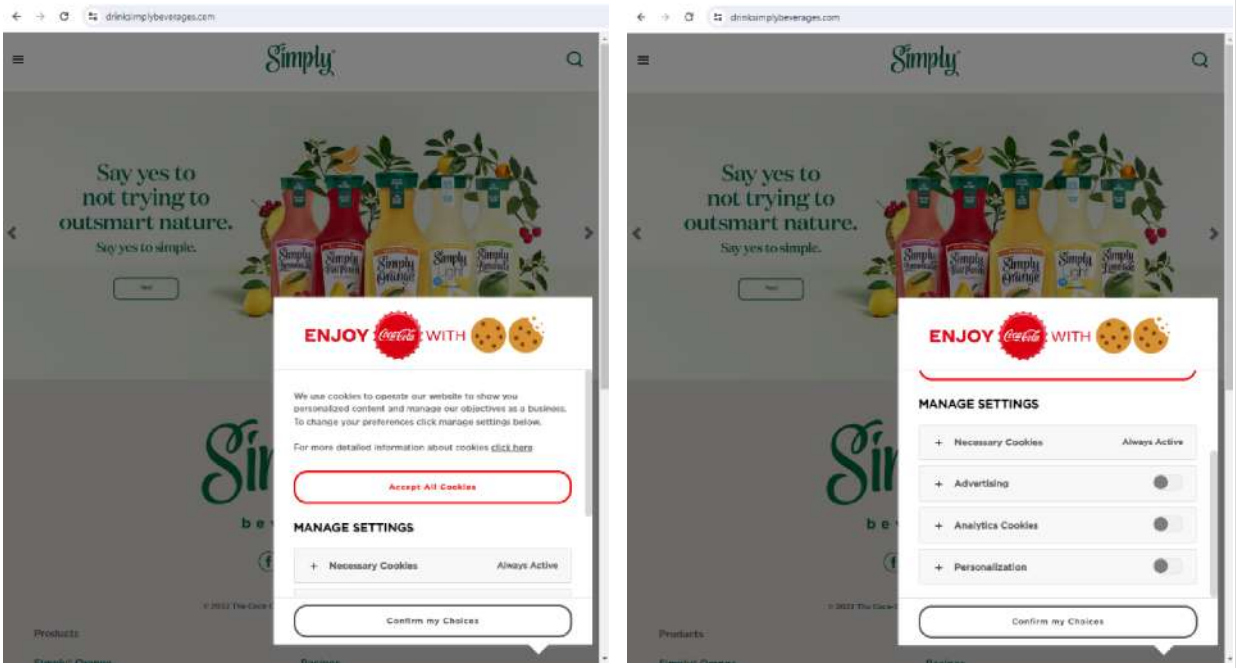


h. From the Fairlife Website:

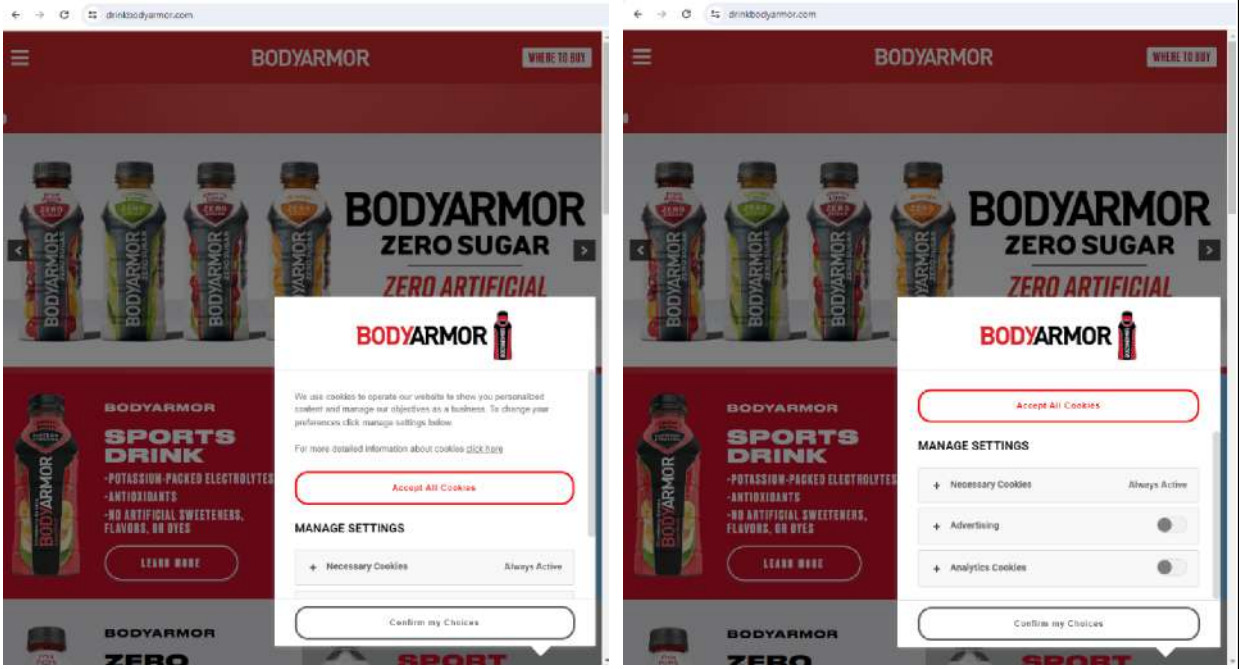




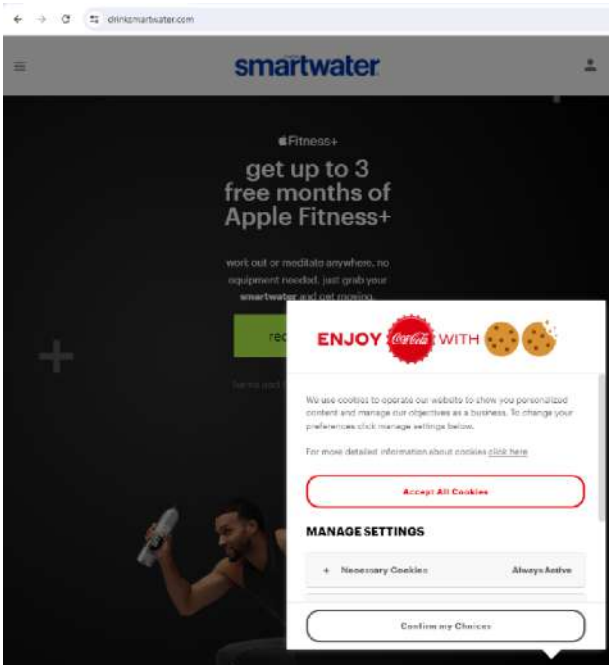
i. From the Simply Website:

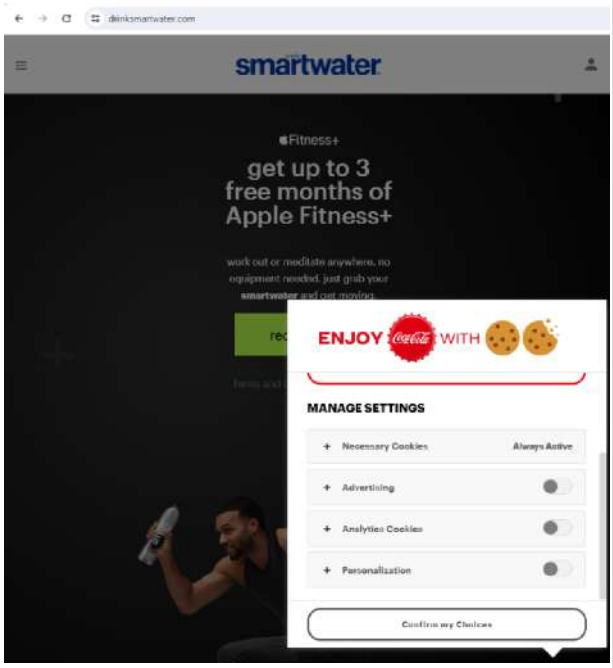


j. From the BODYARMOR Website:



k. From the Smartwater Website:





33. On all the Websites, when users scrolled down in the popup cookie consent banner, they were, in accordance with Defendant's other representations, given the apparent option to manage their cookie settings to decline, reject, or opt out of all cookies for "Advertising," "Analytics," and "Personalization," by adjusting toggle switches associated with each category of cookies.

34. On all the Websites, Defendant informed consumers that they could manage their settings to decline, reject, or opt out of all Advertising, Analytics, and Personalization cookies, which Defendant described as follows:[3]

a. Advertising Cookies: "These cookies are set by us and/or our partners and help us build a profile of your interests based on your browsing profile. If you accept these cookies, you will be shown Coca-Cola advertisements that match your interests as you browse other sites."

[3] Users could view these descriptions by clicking or selecting the "+" symbol that appeared next to each named category of cookies.

b. Analytics Cookies: "These cookies gather information such as how many users are using our site or which pages are popular to help us improve user experience. Switching off these cookies means we can't gather information to improve the experience."

c. Personalization Cookies: "These cookies help us personalize your experience on our site with features like relevant content (e.g. videos) or products you could be interested [in] (e.g. based on what you previously viewed). These cookies will be set by us or by third party providers who add services/features to our sites (e.g. videos)."

35. Plaintiffs and other users of the Websites who adjusted the available toggle switches for all unnecessary cookies, including the categories of Advertising, Analytics, and Personalization cookies, thereby indicating their choice and/or agreement to decline, reject, or opt out of *all* Advertising, Analytics, and Personalization cookies and tracking technologies in use on the Websites, except those "Necessary" for the Websites to function, could then continue to browse the Websites, as the popup cookie consent banner disappeared.

36. Defendant's popup cookie consent banner led Plaintiffs, and all those users of the Websites similarly situated, to believe that they declined, rejected, or opted out of *all* Advertising, Analytics, and Personalization cookies and tracking technologies on the Websites (except those "Necessary" for the Websites to function), especially those used for or associated with advertising, analytics, and personalization functions and content, including those cookies used "to show [users] personalized content and manage [Defendant's] objectives as a business." The banner further reasonably led Plaintiffs and similarly situated users of the Websites to believe that Defendant would not allow third parties, through cookies, to access their Private Communications with the Websites, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, upon adjusting the available toggle switches to decline, reject, or opt out of *all* unnecessary cookies, including Advertising, Analytics, and Personalization cookies.

37. Defendant's representations, however, were false. In truth, Defendant did not abide by Plaintiffs' or other users' wishes. When Plaintiffs and other users of the Websites

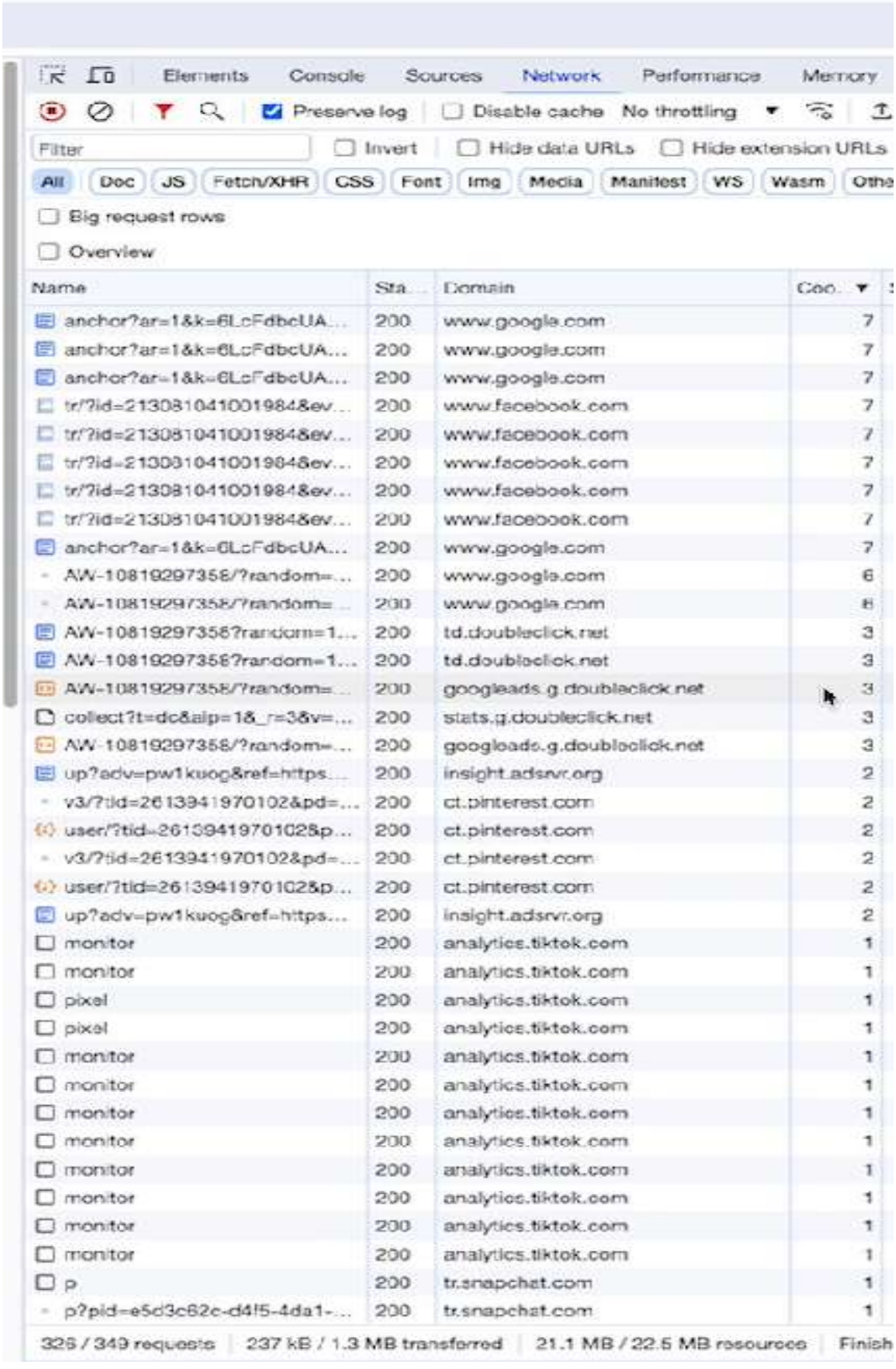
adjusted the available toggle switches to decline, reject, or opt out of all unnecessary cookies, including the categories of Advertising, Analytics, and Personalization cookies, they provided notice to Defendant that they did not consent to the placement or transmission of third-party cookies that would allow those parties to obtain their Private Communications with the Websites.

38. Nevertheless, even after receiving that notice, Defendant causes third-party tracking cookies, including the Third Parties' cookies, to be placed on users' browsers and devices and/or intercepted by the Third Parties, which enabled the Third Parties to collect user data in real time that discloses visitors' Private Communications, including browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. In other words, even when consumers like Plaintiffs tried to protect their privacy by declining, rejecting, or opting out of cookies, Defendant caused cookies to be intercepted by the Third Parties, enabling them to track user behavior and communications.

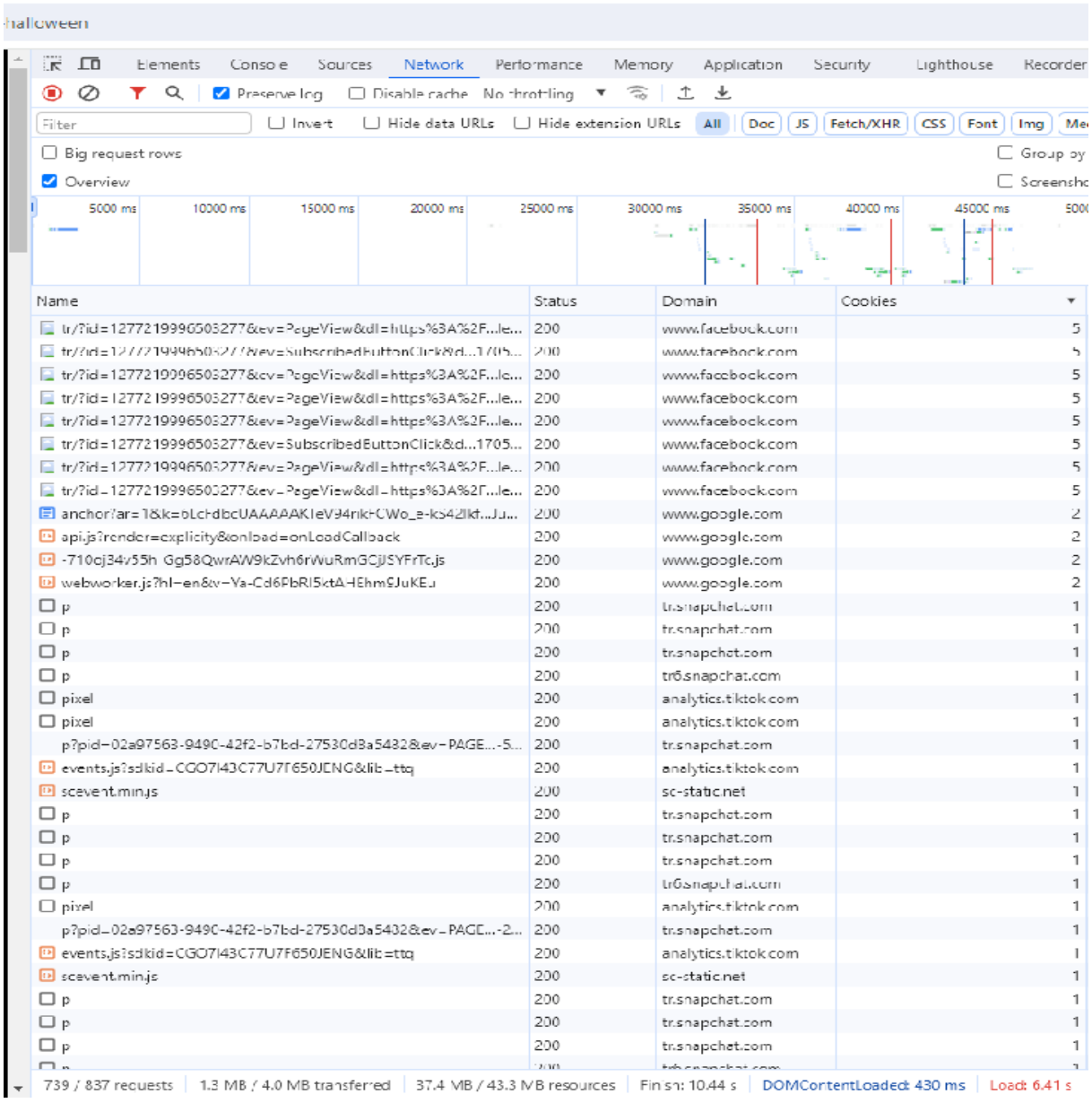
39. Some aspects of the operations of the Third Parties' cookies on the Websites can be observed using specialized tools that log incoming and outgoing network transmissions on the Websites. The following screenshots, obtained using one such tool, show examples of the Third Parties' cookies being transmitted from a user's device and browser to Third Parties on each of Defendant's Websites, even after the user adjusted the available toggle switches to decline, reject, or opt out of all such cookies on each Website's popup cookie consent banner.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

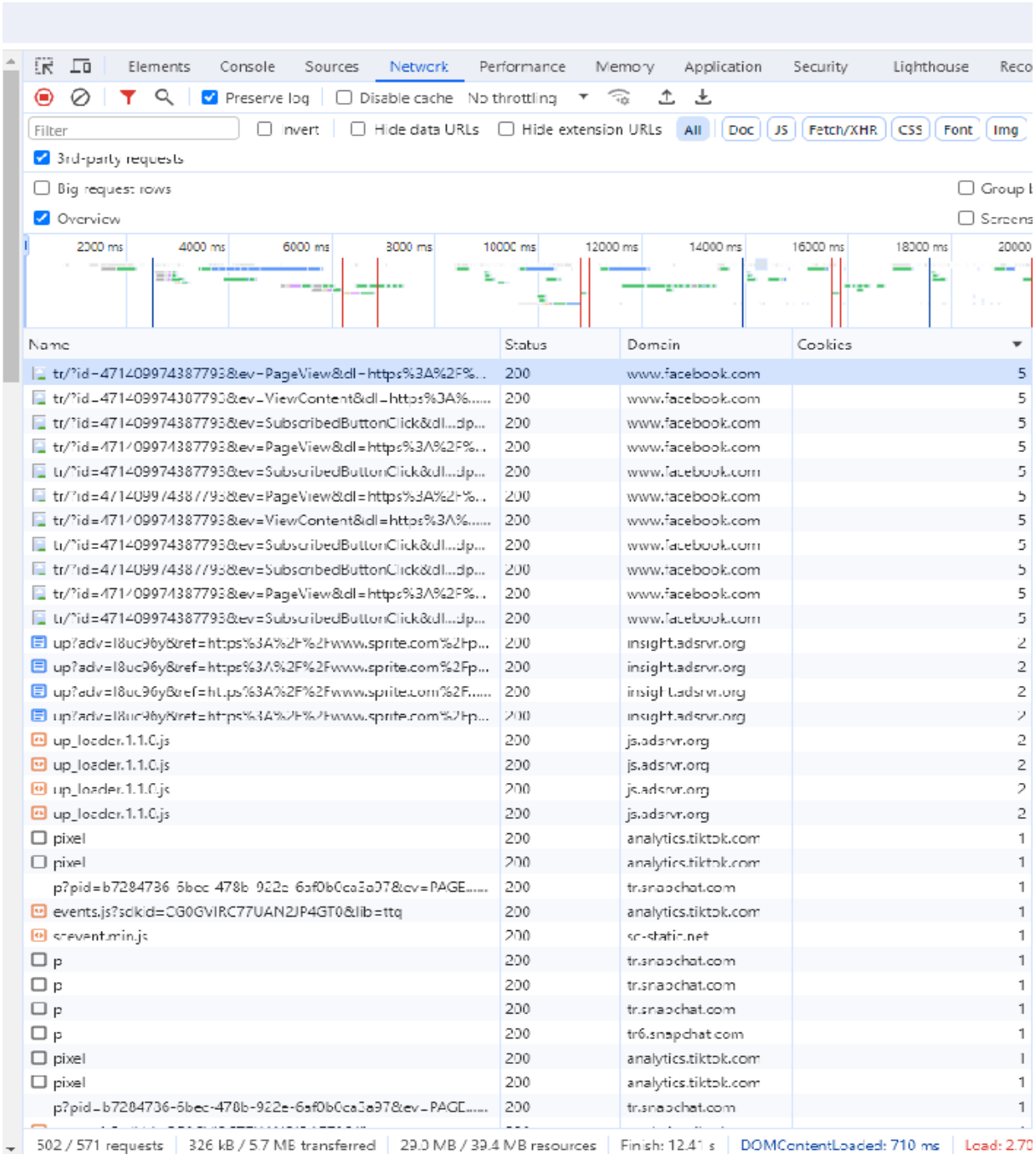
a. From the Coca-Cola Website:



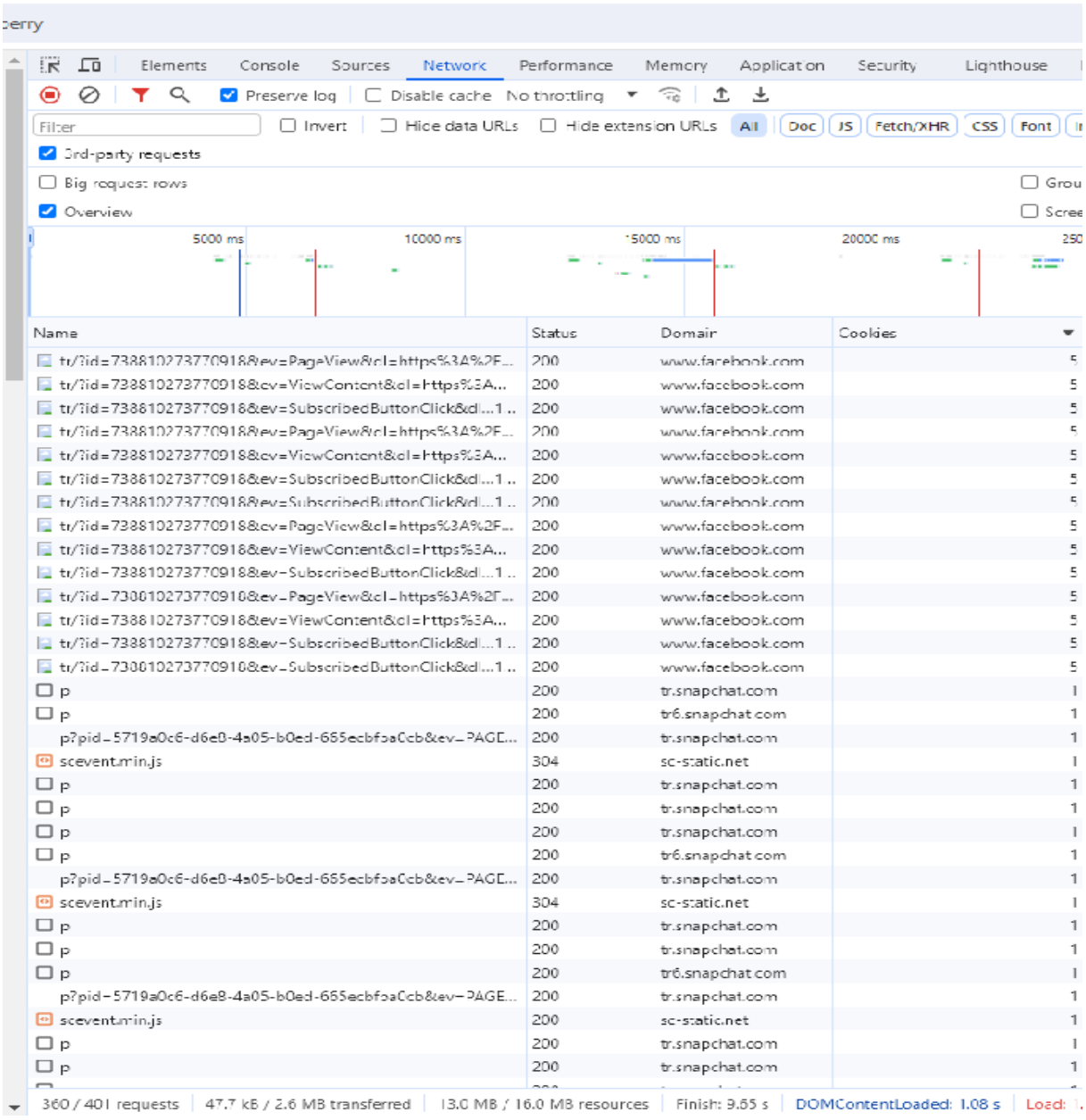
b. From the Fanta Website:



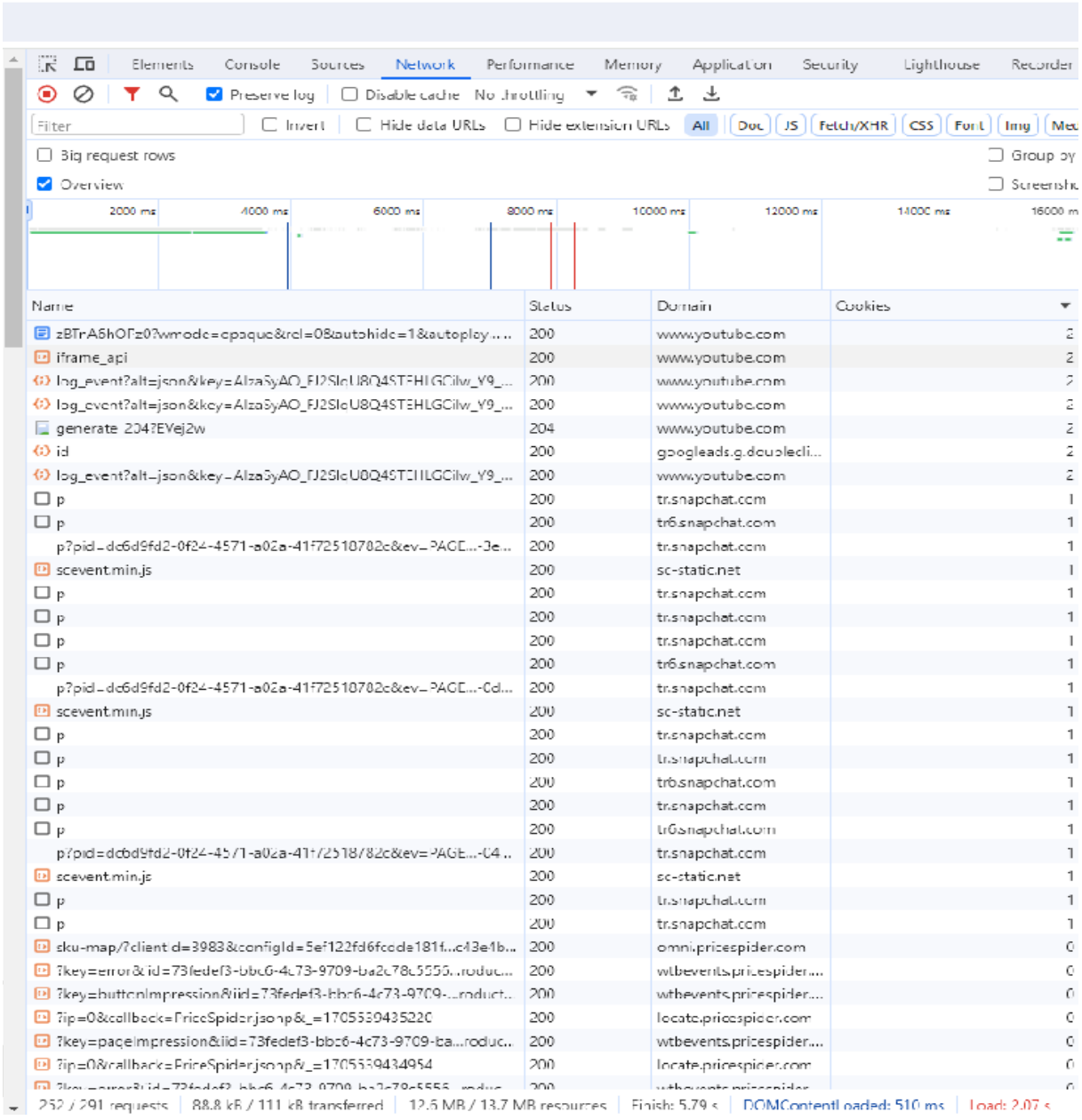
c. From the Sprite Website:



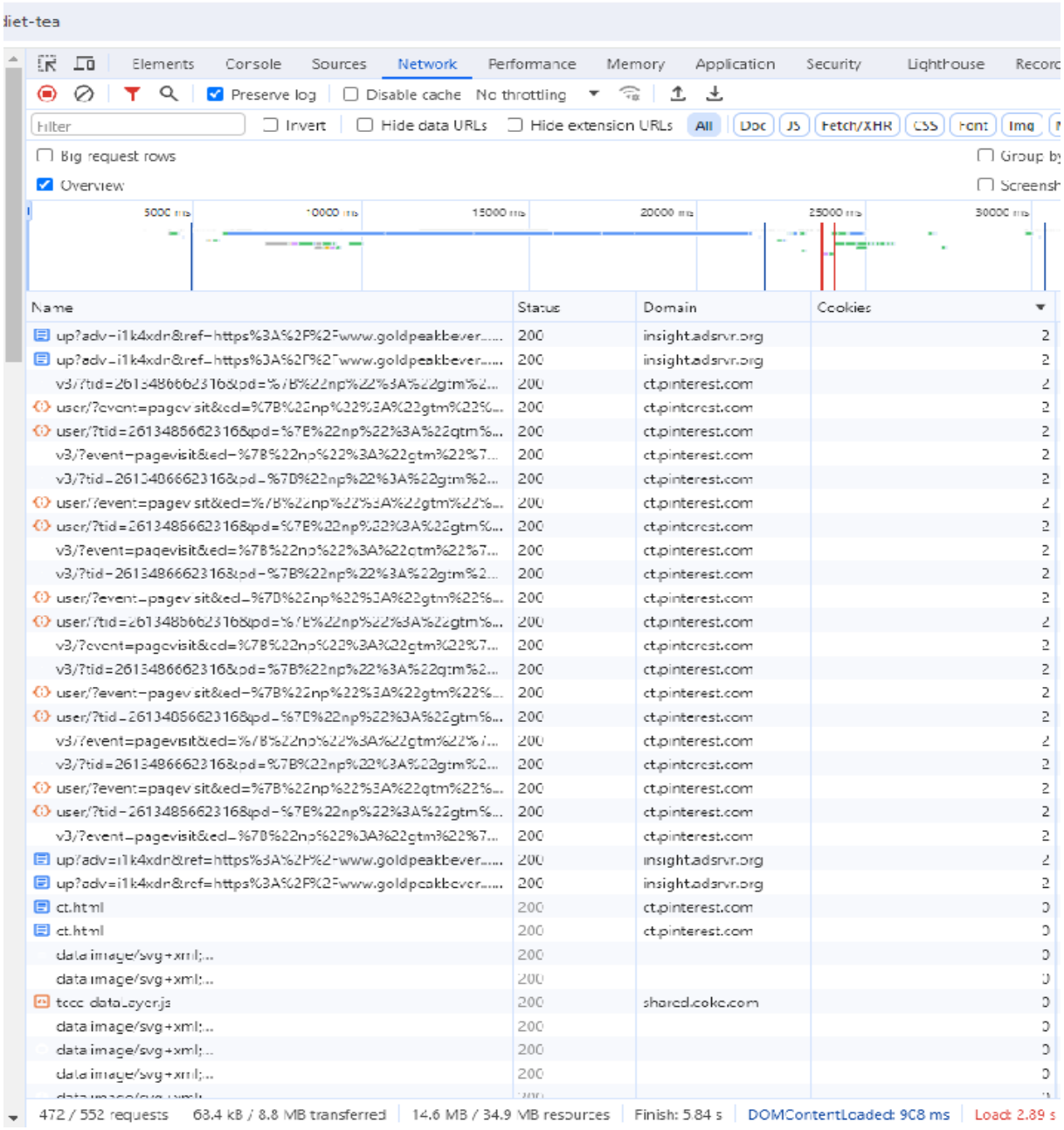
d. From the Powerade Website:



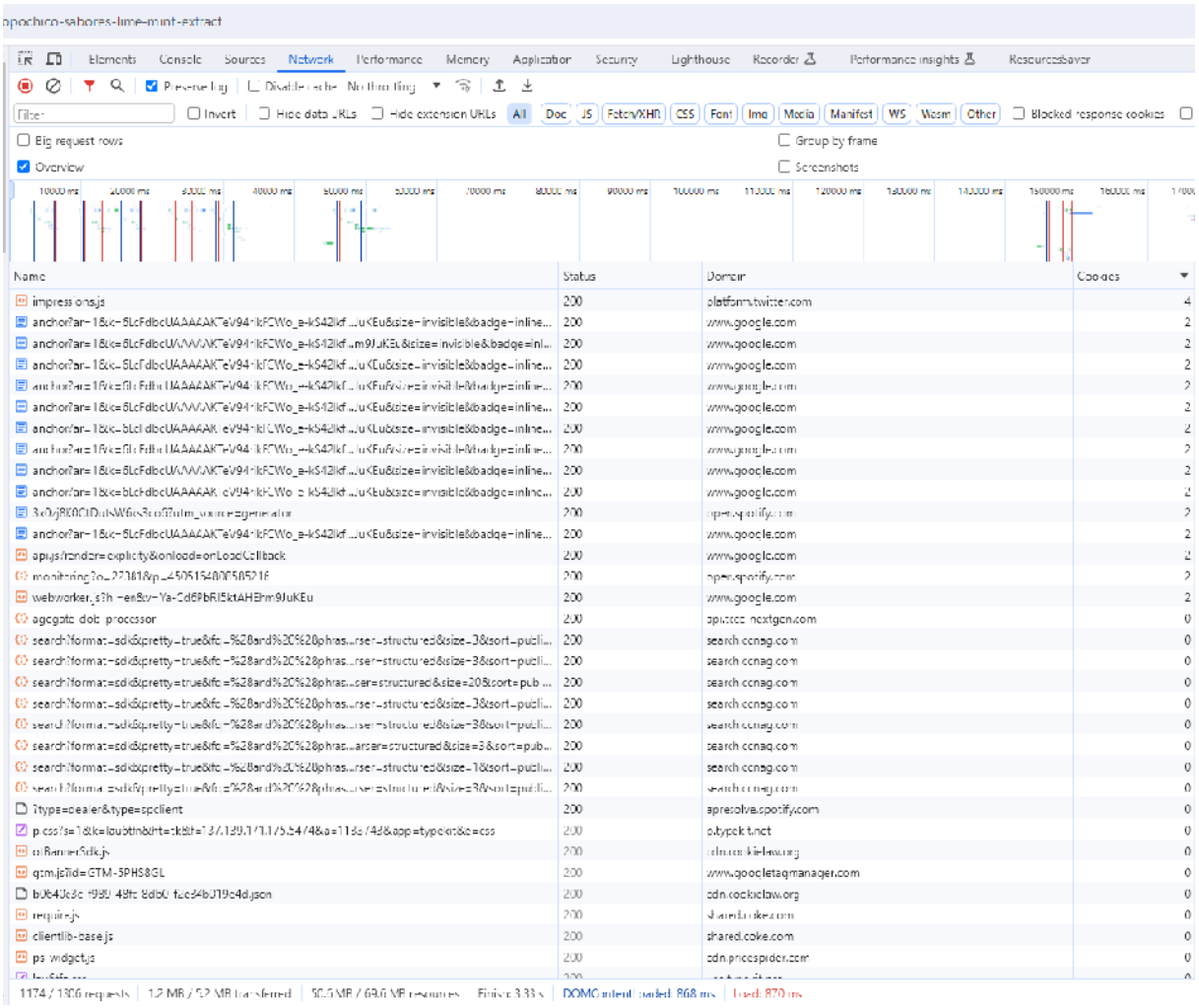
e. From the Diet Coke Website:



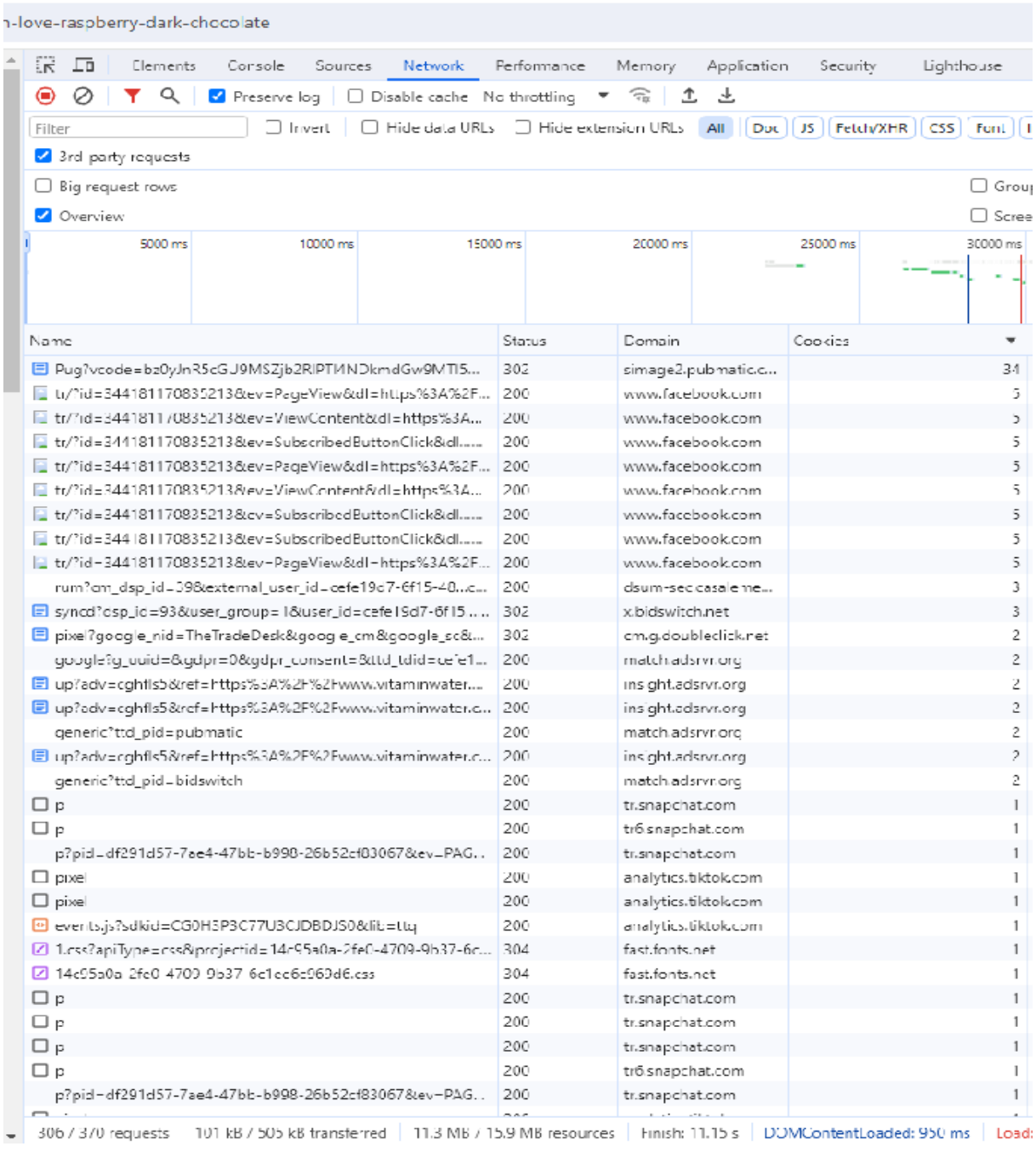
f. From the Gold Peak Website:



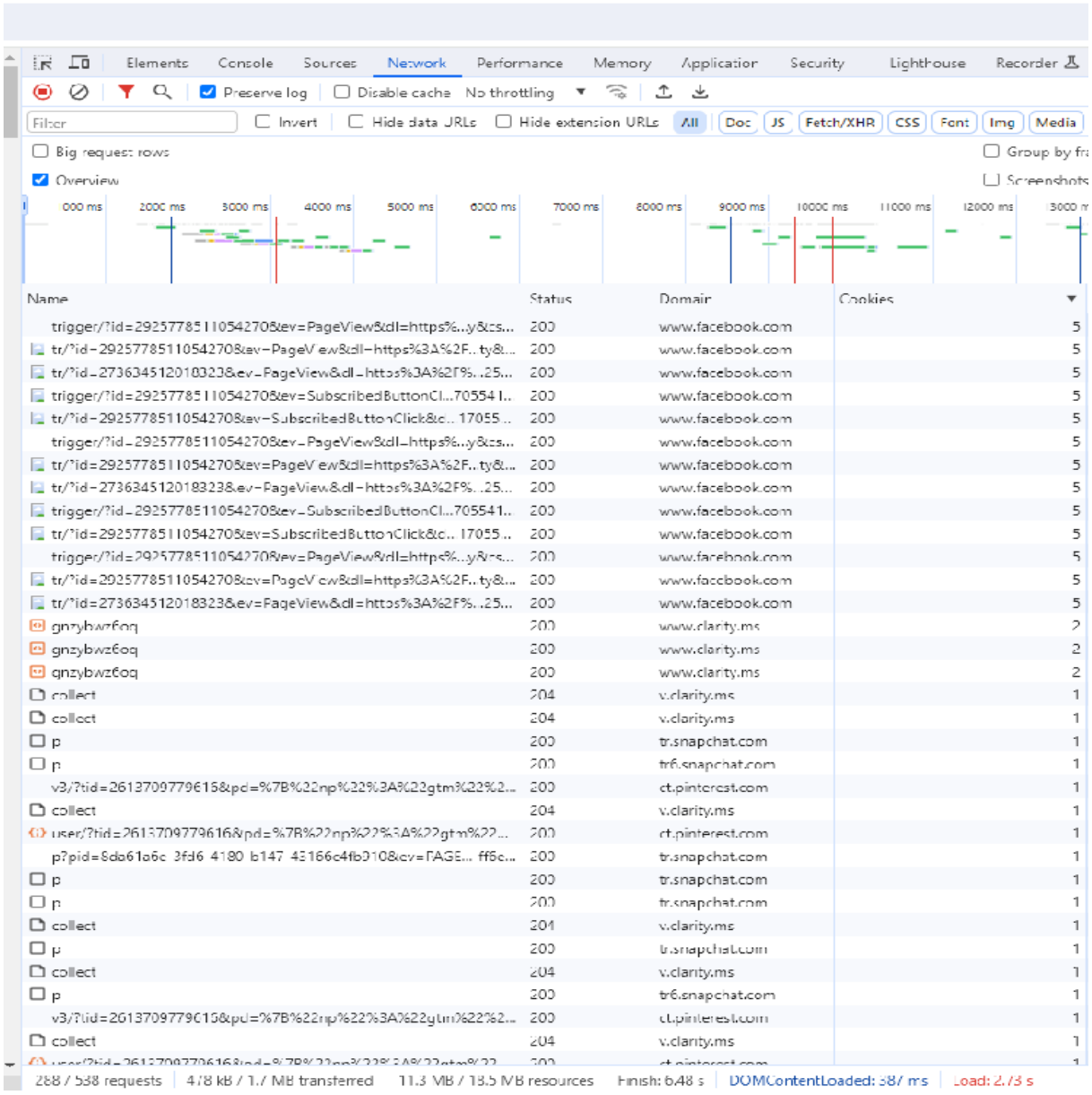
g. From the Topo Chico Website:



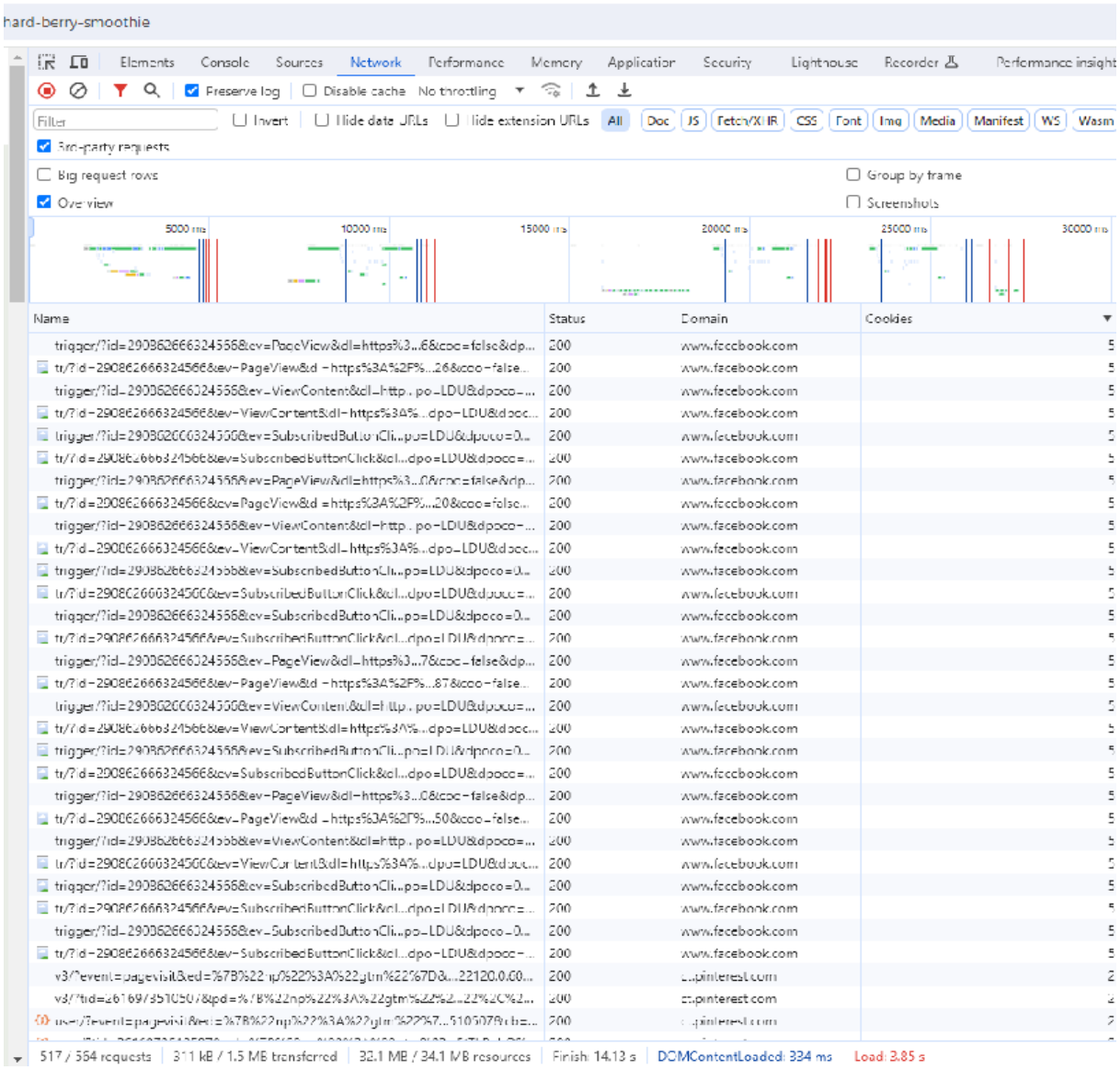
h. From the Vitaminwater Website:



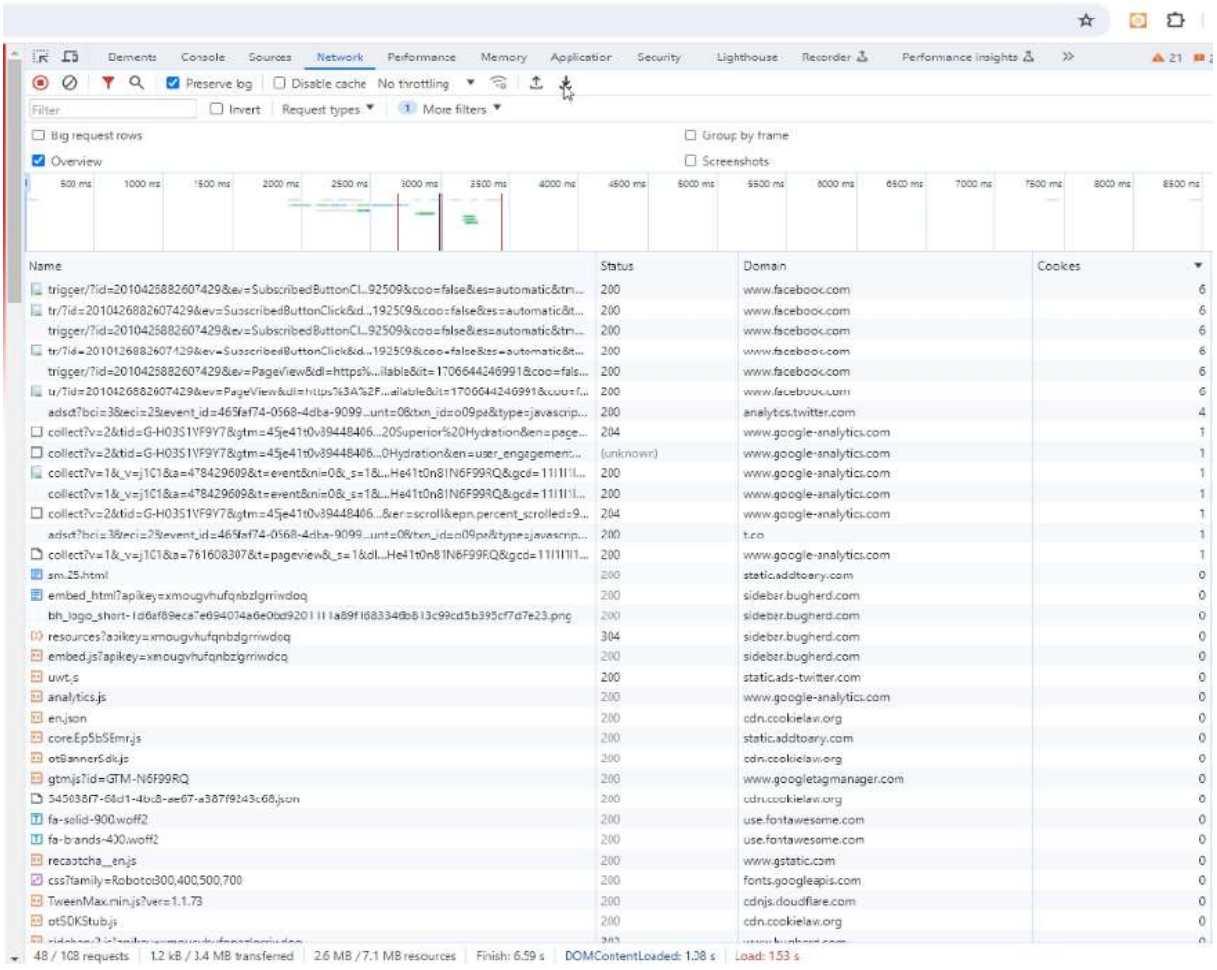
i. From the Fairlife Website:



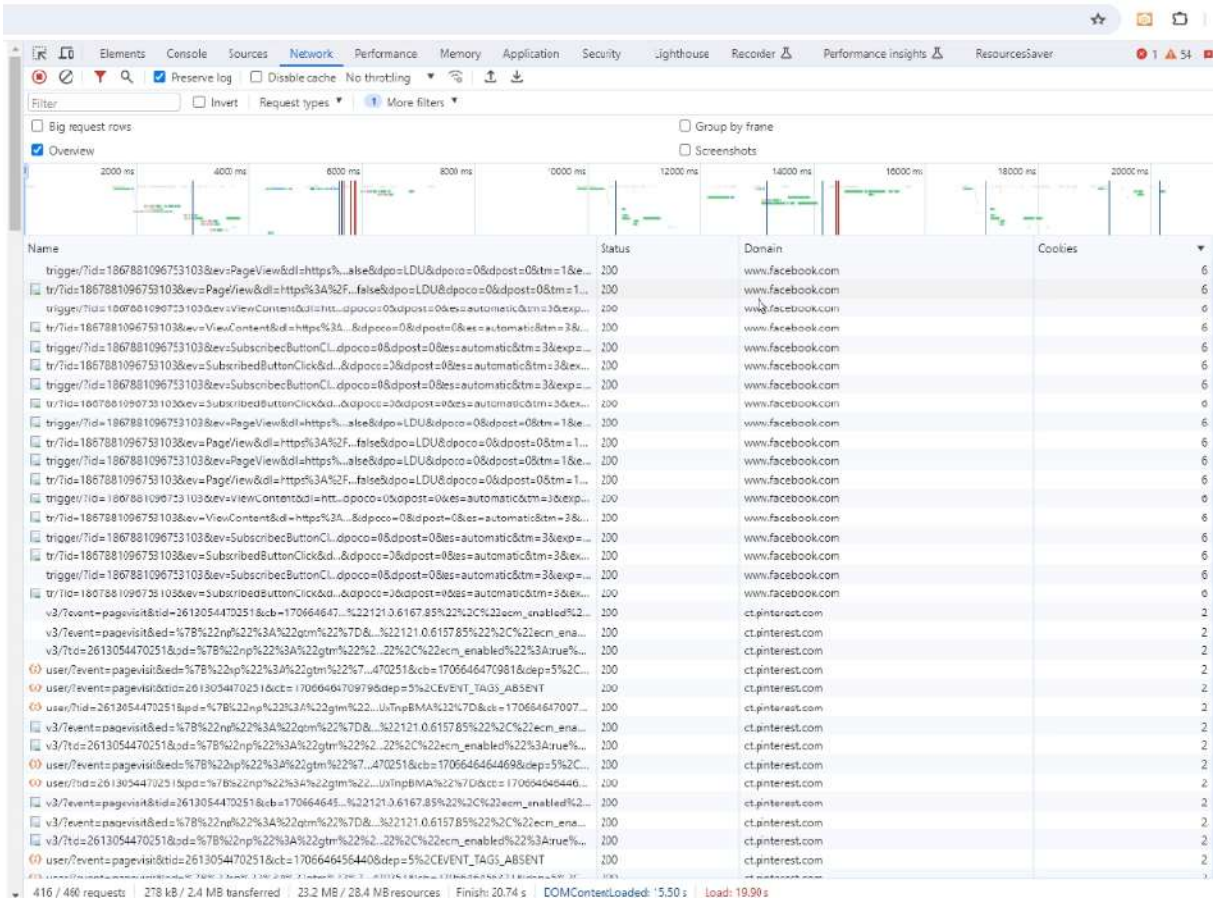
j. From the Simply Website:



k. From the BODYARMOR Website:



1. From the Smartwater Website:



40. The screenshots above show the "Network" tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user's browser and various third-party websites while the user visited and interacted with each of Defendant's Websites. The screenshots depict only network traffic occurring ***after*** the user adjusted the available toggle switches to decline, reject, or opt out of all such cookies using the cookie banner. As shown above, despite the user's rejection of all such cookies, the user's interactions with each of the Websites resulted in the user's browser making a large number of GET and POST HTTP requests to third-party web domains like www.facebook.com, www.google.com, analytics.tiktok.com, and others. As further shown in the right-hand column of the screenshots, the user's browser sent cookies along with those HTTP requests to the third parties on each of the Websites. These screenshots demonstrate that the Websites caused third-party cookie data and users' Private Communications to be intercepted by the Third Parties, even after consumers

adjusted the available toggle switches to decline, reject, or opt out of all unnecessary cookies and tracking technologies, including Advertising, Analytics, and Personalization cookies. All of these network calls are made to the Third Parties without the user's knowledge, and despite the user's rejection of all such cookies.

41. Plaintiffs' and other users' Private Communications with the Websites, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, were surreptitiously obtained by the Third Parties via these cookies.

42. As users interact with the Websites, even after adjusting the toggle switches to decline, reject, or opt out of all unnecessary cookies, including Advertising, Analytics, and Personalization cookies, more data regarding users' behavior and communications are intercepted by the Third Parties, alongside the cookie data. The third-party cookies that Defendant wrongfully allows to be stored on users' devices and browsers, and to be intercepted by the Third Parties, cause the Third Parties to track and collect data on users' behaviors and communications, including Private Communications, on the Websites. Because third-party cookies cause the Third Parties to track users' behavior across the internet and across time, user data can be correlated and combined with other data sets to compile comprehensive user profiles that reflect consumers' behavior, preferences, and demographics (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes). These Third Parties monetize user profiles for advertising, sales, and marketing purposes to generate revenue and target advertising to internet users. Advertisers can gain deep understanding of users' behavioral traits and characteristics and target those users with advertisements tailored to their consumer profiles and audience segments.

43. The third-party code that the Websites cause to be loaded and executed by users' browsers constitutes a wiretap because, when it is executed, it causes the Third Parties—separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. When the

Third Parties use their respective wiretaps on the Websites' users' Private Communications, the wiretaps are not like tape recorders or "tools" used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

C. The Private Communications Intercepted and Collected Through Third-Party Cookies on Defendant's Websites.[4]

1. Meta Cookies (Coca-Cola, Fairlife, BODYARMOR, Powerade, Fanta, Sprite, Vitaminwater, Simply, and Smartwater Websites).

44. Defendant causes third-party cookies to be transmitted between the Websites' users' browsers and devices and the **facebook.com** domain, even after users elect to adjust the available toggle switches to decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies (except those "Necessary Cookies" needed for the Websites to function). This domain is associated with Meta's digital advertising and analytics platform that collects user information via cookies to assist Meta in performing data collection, behavioral analysis, user retargeting, and analytics.[5] Meta serves targeted ads to web users across Meta's ad network, which spans millions of websites and apps.

45. Meta's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. For example, the Coca-Cola Website causes the following data to be sent to Meta when a user browses the Website, even after the user has rejected all Advertising, Analytics, and Personalization cookies:

[4] This section contains multiple examples of specific data being sent from a user's browser to third parties. Each example was collected after the user had chosen to opt-out of or reject all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies (except those "Necessary Cookies" needed for the Websites to function).

[5] Meta Cookies Policy (available at https://www.facebook.com/privacy/policies/cookies/).

GET 200 https://www.facebook.com/tr/?id=213081041001984&ev=PageFus.coca-cola.com%2Fproducts%2Fcoca-cola&if=false&ts=16b.1.1699914231361.89312336&ler=empty&it=1699914363696&c

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	www.facebook.com
:method	GET
:path	/tr/?id=213081041001984&ev=PageView&dl=https%3A%2F%2Fus.coca-cola.com%2Fproducts%2Fcoca-cola%2Foriginal&rl=https%3A%2F%2Fus.coca-cola.com%2Fproducts%2Fcoca-cola&if=false&ts=1699914363760&sw=2240&sh=1260&v=2.9.138&r=stable&a=tmSimo-GTM-WebTemplate&ec=0&o=4126&fbp=fb.1.1699914231361.89312336&ler=empty&it=1699914363696&coo=false&dpo=LDU&dpoco=0&dpost=0&tm=1&rqm=GET
:scheme	https
accept	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
cookie	sb=fOVLZR0Xt0o9N5_8p_wZ5MjR; datr=fOVLZfR2FfnjjsD4-tymrtuF; locale=en_US; c_user=1345507951; dpr=2; xs=9%3AnDPKrgBzIw1grQ%3A2%3A1699472819%3A-1%3A2633%3A%3AAcXIJK6CxgLqP7lH8tmcOFrMxkwq4C1Gg0F11DduZg; fr=1wOAnjTbJIFh3ZURe.AWV8OTt4OhEi1aUvBbI1ACH195U.BlUdad.Hj.AAA.0.0.BlUdad.AWVD4eQukCA
Host	www.facebook.com
referer	https://us.coca-cola.com/
sec-ch-ua	"Google Chrome";v="119", "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
sec-fetch-dest	image
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36

GET 200 https://www.facebook.com/tr/?id=213081041001984&ev=PageFus.coca-cola.com%2Fproducts%2Fcoca-cola&if=false&ts=16b.1.1699914231361.89312336&ler=empty&it=1699914363696&c

Request Header Query Body Cookies Raw Summary +

Key	Value
a	tmSimo-GTM-WebTemplate
coo	false
dl	https://us.coca-cola.com/products/coca-cola/original
dpo	LDU
dpoco	0
dpost	0
ec	0
ev	PageView
fbp	fb.1.1699914231361.89312336
id	213081041001984
if	false
it	1699914363696
ler	empty
o	4126
r	stable
rl	https://us.coca-cola.com/products/coca-cola
rqm	GET
sh	1260
sw	2240
tm	1
ts	1699914363760
v	2.9.138

GET 200 https://www.facebook.com/tr/?id=213081041001984&ev=PageFus.coca-cola.com%2Fproducts%2Fcoca-cola&if=false&ts=16b.1.1699914231361.89312336&ler=empty&it=1699914363696&c

Request Header Query Body Cookies Raw Summary +

Key	Value
c_user	1345507951
datr	fOVLZfR2FfnjjsD4-tymrtuF
dpr	2
fr	1wOAnjTbJIFh3ZURe.AWV8OTt4OhEi1aUvBbI1ACH195U.BlUdad.Hj.AAA.0.0.BlUdad.AWVD4eQukCA
locale	en_US
sb	fOVLZR0Xt0o9N5_8p_wZ5MjR
xs	9%3AnDPKrgBzlw1grQ%3A2%3A1699472819%3A-1%3A2633%3A%3AAcXlJK6CxgLqP7IH8tmcOFrMxkwq4C1Gg0F11DduZg

46. Similarly, the following type of data is sent to Meta when a user browses the Fairlife Website:

GET 200 https://www.facebook.com/privacy_sandbox/pixel/register-shake%2F&rl=https%3A%2F%2Ffairlife.com%2Fcore-power%2F1697249.1178022563&ler=empty&cs_est=true&it=17055417596

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	www.facebook.com
:method	GET
:path	/privacy_sandbox/pixel/register/trigger/?id=2925778511054270&ev=PageView&dl=https%3A%2F%2Ffairlife.com%2Fvanilla-protein-shake%2F&rl=https%3A%2F%2Ffairlife.com%2Fcore-power%2F&if=false&ts=1705541760362&sw=1920&sh=1080&v=2.9.140&r=stable&ec=0&o=4126&fbp=fb.1.1705541697249.1178022563&ler=empty&cs_est=true&it=1705541759661&coo=false&rqm=FGET
:scheme	https
accept	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
attribution-reporting-eligible	trigger, event-source
cookie	sb=63-oZXb-WgN5xgNLUBEcBVpd; datr=63-oZaBPlkRkU98oiLT4BIVX; c_user=100076133960803; xs=46%3AtE0mlO9SHP9aPA%3A2%3A1705541614%3A-1%3A-1; fr=0uriwMMnaJf16x1Pg.AWUsOmivE86TZ4F63M_S-u0yfOM.BlqH_r.Ak.AAA.0.0.BlqH_v.AWVAUWNzCBI
Host	www.facebook.com
priority	u=3, i
referer	https://fairlife.com/
sec-ch-ua	"Not_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"Windows"
sec-fetch-dest	image
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

GET 200 https://www.facebook.com/privacy_sandbox/pixel/register-shake%2F&rl=https%3A%2F%2Ffairlife.com%2Fcore-power%2F1697249.1178022563&ler=empty&cs_est=true&it=17055417596

Request Header Query Body Cookies Raw Summary +

Key	Value
coo	false
cs_est	true
dl	https://fairlife.com/vanilla-protein-shake/
ec	0
ev	PageView
fbp	fb.1.1705541697249.1178022563
id	2925778511054270
if	false
it	1705541759661
ler	empty
o	4126
r	stable
rl	https://fairlife.com/core-power/
rqm	FGET
sh	1080
sw	1920
ts	1705541760362
v	2.9.140

GET 200 https://www.facebook.com/privacy_sandbox/pixel/register-shake%2F&rl=https%3A%2F%2Ffairlife.com%2Fcore-power%2F1697249.1178022563&ler=empty&cs_est=true&it=17055417596

Request Header Query Body Cookies Raw Summary +

Key	Value
c_user	100076133960803
datr	63-oZaBPlkRkU98oiLT4BlVX
fr	0uriwMMnaJf16x1Pg.AWUsOmivE86TZ4F63M_S-u0yfOM.BlqH_r.Ak.AAA.0.0.BlqH_v.AWVAUWNzCBI
sb	63-oZXb-WgN5xgNLUBEcBVpd
xs	46%3AtE0mlO9SHP9aPA%3A2%3A1705541614%3A-1%3A-1

47. Similarly, the following type of data is sent to Meta when a user browses the BODYARMOR Website:

GET 200 https://www.facebook.com/privacy_sandbox/pixel/register
ct%2Fstrawberry-banana%2F&rl=https%3A%2F%2Fwww.drinkbod
&ec=0&o=4126&fbp=fb.1.1706644142483.603330015&ler=empty

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	www.facebook.com
:method	GET
:path	/privacy_sandbox/pixel/register/trigger/?id=2010426882607429&ev=PageView&dl=https%3A%2F%2Fwww.drinkbodyarmor.com%2Fproduct%2Fstrawberry-banana%2F&rl=https%3A%2F%2Fwww.drinkbodyarmor.com%2Fsports-drink%2F&if=false&ts=1706644265289&sw=1920&sh=1080&v=2.9.143&r=stable&ec=0&o=4126&fbp=fb.1.1706644142483.603330015&ler=empty&cdl=API_unavailable&it=1706644265062&coo=false&exp=e1&rqm=FGET
:scheme	https
accept	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
attribution-reporting-eligible	trigger, event-source=navigation-source
cookie	ps_n=0; sb=_1C5ZYwOdm6EROxmP-RQAqn_; datr=_1C5ZSpxfSuNIIMkhyDtji8b; c_user=100076133960803; xs=31%3AmJLvEILSHHJ_8Q%3A2%3A1706643719%3A-1%3A-1; fr=0v5L2MBR12qFe4vJI.AWWwoi_G_7IPOIFuSMMpwP4ZQSM.BluVD_.Hc.AAA.0.0.BluVEJ.AWWj7sVviCY
Host	www.facebook.com
priority	u=3, i
referer	https://www.drinkbodyarmor.com/
sec-ch-ua	"Not A(Brand";v="99", "Google Chrome";v="121", "Chromium";v="121"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"Windows"
sec-fetch-dest	image
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

GET 200 https://www.facebook.com/privacy_sandbox/pixel/register
ct%2Fstrawberry-banana%2F&rl=https%3A%2F%2Fwww.drinkbod
&ec=0&o=4126&fbp=fb.1.1706644142483.603330015&ler=empty

Request Header Query Body Cookies Raw Summary +

Key	Value
cdl	API_unavailable
coo	false
dl	https://www.drinkbodyarmor.com/product/strawberry-banana/
ec	0
ev	PageView
exp	e1
fbp	fb.1.1706644142483.603330015
id	2010426882607429
if	false
it	1706644265062
ler	empty
o	4126
r	stable
rl	https://www.drinkbodyarmor.com/sports-drink/
rqm	FGET
sh	1080
sw	1920
ts	1706644265289
v	2.9.143

GET 200 https://www.facebook.com/privacy_sandbox/pixel/register
ct%2Fstrawberry-banana%2F&rl=https%3A%2F%2Fwww.drinkbod
&ec=0&o=4126&fbp=fb.1.1706644142483.603330015&ler=empty

Request Header Query Body Cookies Raw Summary +

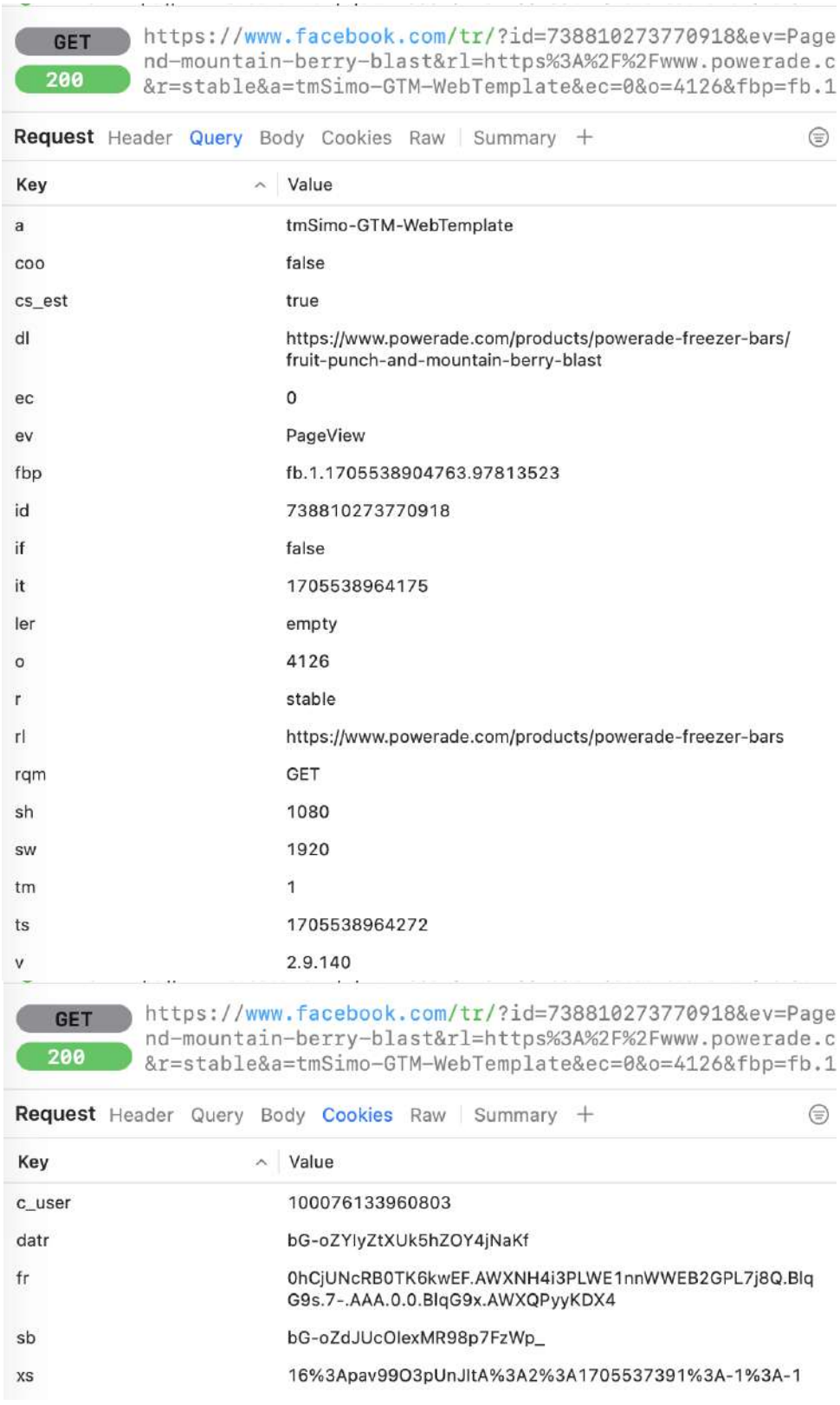
Key	Value
c_user	100076133960803
datr	_1C5ZSpxfSuNIIMkhyDtji8b
fr	0v5L2MBR12qFe4vJl.AWWwoi_G_7lPOlFuSMMpwP4ZQSM.BluV D_.Hc.AAA.0.0.BluVEJ.AWWj7sVviCY
ps_n	0
sb	_1C5ZYwOdm6EROxmP-RQAqn_
xs	31%3AmJLvEILSHHJ_8Q%3A2%3A1706643719%3A-1%3A-1

48. Similarly, the following type of data is sent to Meta when a user browses the Powerade Website:

GET 200 https://www.facebook.com/tr/?id=738810273770918&ev=Page nd-mountain-berry-blast&rl=https%3A%2F%2Fwww.powerade.c &r=stable&a=tmSimo-GTM-WebTemplate&ec=0&o=4126&fbp=fb.1

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	www.facebook.com
:method	GET
:path	/tr/?id=738810273770918&ev=PageView&dl=https%3A%2F%2Fwww.powerade.com%2Fproducts%2Fpowerade-freezer-bars%2Ffruit-punch-and-mountain-berry-blast&rl=https%3A%2F%2Fwww.powerade.com%2Fproducts%2Fpowerade-freezer-bars&if=false&ts=1705538964272&sw=1920&sh=1080&v=2.9.140&r=stable&a=tmSimo-GTM-WebTemplate&ec=0&o=4126&fbp=fb.1.1705538904763.97813523&cs_est=true&ler=empty&it=1705538964175&coo=false&tm=1&rqm=GET
:scheme	https
accept	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
cookie	sb=bG-oZdJUcOlexMR98p7FzWp_; datr=bG-oZYlyZtXUk5hZOY4jNaKf; c_user=100076133960803; xs=16%3Apav99O3pUnJltA%3A2%3A1705537391%3A-1%3A-1; fr=0hCjUNcRB0TK6kwEF.AWXNH4i3PLWE1nnWWEB2GPL7j8Q.BlqG9s.7-.AAA.0.0.BlqG9x.AWXQPyyKDX4
Host	www.facebook.com
priority	u=3, i
referer	https://www.powerade.com/products/powerade-freezer-bars/fruit-punch-and-mountain-berry-blast
sec-ch-ua	"Not_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"Windows"
sec-fetch-dest	image
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36



GET
200
https://www.facebook.com/tr/?id=738810273770918&ev=Page
nd-mountain-berry-blast&rl=https%3A%2F%2Fwww.powerade.c
&r=stable&a=tmSimo-GTM-WebTemplate&ec=0&o=4126&fbp=fb.1

Request Header Query Body Cookies Raw Summary +

Key	Value
a	tmSimo-GTM-WebTemplate
coo	false
cs_est	true
dl	https://www.powerade.com/products/powerade-freezer-bars/fruit-punch-and-mountain-berry-blast
ec	0
ev	PageView
fbp	fb.1.1705538904763.97813523
id	738810273770918
if	false
it	1705538964175
ler	empty
o	4126
r	stable
rl	https://www.powerade.com/products/powerade-freezer-bars
rqm	GET
sh	1080
sw	1920
tm	1
ts	1705538964272
v	2.9.140

GET
200
https://www.facebook.com/tr/?id=738810273770918&ev=Page
nd-mountain-berry-blast&rl=https%3A%2F%2Fwww.powerade.c
&r=stable&a=tmSimo-GTM-WebTemplate&ec=0&o=4126&fbp=fb.1

Request Header Query Body Cookies Raw Summary +

Key	Value
c_user	100076133960803
datr	bG-oZYlyZtXUk5hZOY4jNaKf
fr	0hCjUNcRB0TK6kwEF.AWXNH4i3PLWE1nnWWEB2GPL7j8Q.BlqG9s.7-.AAA.0.0.BlqG9x.AWXQPyyKDX4
sb	bG-oZdJUcOlexMR98p7FzWp_
xs	16%3Apav99O3pUnJltA%3A2%3A1705537391%3A-1%3A-1

49. The "ev" parameter is an "Event." In this case, the event is a "PageView," indicating to Meta that the user has viewed a specific webpage on the Website.

50. The "dl" parameter is the "Document Location." It tells Meta the specific webpage on which the Event occurred.

51. The "ts" parameter corresponds to a "Timestamp," and tells Meta the exact time—down to the millisecond—at which the user viewed the page.

52. The "fbp" parameter is the Facebook Browser ID, and is used to track the user's activity across the internet.

53. The "c_user" cookie shown above enables Meta to identify a specific user when they are logged in to their account. The "c_user" cookie stores a user's unique ID, which is associated with their Facebook profile. This ID enables Meta to track user interactions on its platform and across sites that use Facebook plugins, such as adding items to a cart, clicking "Like" buttons, or engaging with comment sections. When combined with other data sent to the Facebook domain, this cookie allows Meta to track users' browsing activities. Meta uses this data for various purposes, such as personalizing content, enhancing ad targeting accuracy, and refining its user experience. Cookies enable Meta "to understand the information that [Meta] receive[s] about [users], including information about [users'] use of other websites and apps, whether or not [users] are registered or logged in."[6]

54. Further, as shown above, along with all of this data, the Meta software code that Defendant causes to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to Meta.

55. The "user-agent" corresponds to the device and browser that the user has used to access the Websites.[7]

56. Finally, the data sent to Meta contains the user's IP address.

57. The other Websites that send cookie data to Meta even after users have rejected all unnecessary cookies (i.e., the Fanta, Sprite, Vitaminwater, Simply, and Smartwater Websites) operate in substantially the same way as the Websites described above, with each of those

---

[6] *Id.*

[7] There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at https://explore.whatismybrowser.com/useragents/parse.

Websites sending substantially the same type of header data, query data, and cookie data to Meta even after users have rejected all unnecessary cookies.

58. In particular, by identifying users who have shown interest in certain products or content, the facebook.com cookies enable Meta's advertising platform to show relevant advertisements to users who have demonstrated interest in particular products or content.[8] These cookies allow Meta to collect data on how users interact with websites, regardless of whether they have a Facebook account or are logged in.[9]

59. Cookies allow Meta to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses, which allow Meta to determine whether a user is located in California).[10]

60. Meta utilizes the data collected through the facebook.com cookies for its own purposes, including by using the data to tailor content and target advertisements to users. This includes practices such as (i) Ad Targeting and Retargeting, in which Meta uses the facebook.com cookie to track users' online behavior across different sites, building a profile based on their browsing habits, purchases, and interactions. This profile enables Meta to deliver highly targeted ads within the Facebook ecosystem and on other sites that are part of Facebook's Audience Network; (ii) Conversion Tracking, in which Meta uses the facebook.com cookie to enable business partners to track specific actions users take after viewing or clicking on a Facebook ad, such as making a purchase or signing up for a newsletter; (iii) Audience Insights and Analytics, in which Meta uses the facebook.com cookie to provide data to businesses on user demographics, interests, and behaviors across their sites and apps; and (iv) Cross-Device

---

[8] *Id.*; https://allaboutcookies.org/what-data-does-facebook-collect.
[9] https://allaboutcookies.org/what-data-does-facebook-collect.
[10] Meta Cookies Policy (available at https://www.facebook.com/privacy/policies/cookies); Meta Privacy Policy (available at https://www.facebook.com/privacy/policy/); Customer Information Parameters (available at https://developers.facebook.com/documentation/ads-commerce/conversions-api/parameters/customer-information-parameters); Advanced matching – Meta Pixel (available at https://developers.facebook.com/documentation/meta-pixel/advanced/advanced-matching); https://allaboutcookies.org/what-data-does-facebook-collect.

and Cross-Platform Tracking, in which Meta uses the facebook.com cookie to support tracking users across devices and platforms, so that ads are targeted consistently regardless of the device a user is on. This ensures that advertisers can follow users across devices. Meta also states that "other companies' cookies help tailor ads off of Meta Products, measure their performance and effectiveness and support marketing and analytics."[11]

2. Google Cookies (Coca-Cola, BODYARMOR, and Diet Coke Websites).

61. Defendant causes third-party cookies to be transmitted between the Websites' users' browsers and devices and the **google-analytics.com**; **google.com**; **adservice.google.com**; **googleadservices.com**; **googlesyndication.com**; and **doubleclick.net** domains, even after users elect to adjust the available toggle switches to decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies (except those "Necessary Cookies" needed for the Websites to function). Each of these domains is associated with Google LLC's digital advertising and analytics platform that collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.[12] Website users' browsers automatically send Google their page URL and IP address.[13] Further, the Websites permit Google to set cookies on the Website users' browsers and read cookies that are already there.[14] Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's DoubleClick cookies.[15] Google's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. Further, by identifying users who have shown interest in certain products or content, Google's

[11] Meta Cookies Policy, https://www.facebook.com/privacy/policies/cookies/.
[12] *See* Our advertising and measurement cookies (available at https://business.safety.google/adscookies/).
[13] *See* How Google uses information from sites or apps that use our services (available at http://policies.google.com/technologies/partner-sites).
[14] *Id.*
[15] *See, e.g.,* https://www.ghostery.com/whotracksme/trackers/doubleclick.

cookies allow advertisers to show relevant ads to those users when they visit other websites within Google's ad network.[16]

62. Specifically, Google sends cookies when a web user visits a webpage that shows Google Marketing Platform advertising products and/or Google Ad Manager ads.[17] "Pages with Google Marketing Platform advertising products or Google Ad Manager ads include ad tags that instruct browsers to request ad content from [Google's] servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google Marketing Platform advertising products or Google Ad Manager ads for this to happen; it just needs to include Google Marketing Platform advertising products or Google Ad Manager ad tags, which might load a click tracker or impression pixel instead." *Id.* As Google explains, "Google Marketing Platform advertising products and Google Ad Manager send a cookie to the browser after any impression, click, or other activity that results in a call to our servers." *Id.*

63. Google also uses cookies in performing analytical functions. As Google explains, "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es]."[18] "To measure a website … [one] add[s] a small piece of JavaScript measurement code to each page on [a] site." *Id.* Then, "[e]very time a user visits a webpage, the tracking code will collect … information about how that user interacted with the page." *Id.* Google Analytics enables website owners to "measure when someone loads a page, clicks a link," "completes a purchase"; "searches … website or app"; "select[s] content on … [a] website or app"; "views an item"; and "views their shopping cart."[19]

---

[16] *See, e.g.,* About cross-channel remarketing in Search Ads 360 (available at https://support.google.com/searchads/answer/7189623?hl=en); About dynamic remarketing for retail (available at https://support.google.com/google-ads/answer/6099158?hl=en&sjid=11962135750754589 08-NC).

[17] *See* How Google Marketing Platform advertising products and Google Ad Manager use cookies (available at https://support.google.com/searchads/answer/2839090?hl=en&sjid=11962135750754589 08-NC); *see also* Cookies and user identification (available at https://developers.google.com/tag-platform/security/concepts/cookies).

[18] How Google Analytics Works (available at https://support.google.com/analytics/answer/12159447?hl=en).

[19] Set up events (available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://developers.google.com/analytics/devguides/collection/ga4/events).

64. Google's cookies allow it to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data—including whether a user is located in California.[20]

65. Google's own Privacy & Terms materials provide that Google "store[s] a record of the ads … serve[d] in [its] logs."[21] "These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser or, if you are signed-in, that may uniquely identify you."[22] Google then uses location information to infer the Website users' demographic information.[23]

66. For example, the Google software code that Defendant causes to be stored on and executed by the Websites' users' devices causes the following data to be sent to Google's domain, at googleads.g.doubleclick.net, when the user browses the Coca-Cola Website, even after the user has rejected all Advertising, Analytics, and Personalization cookies:

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

---

[20] *See* About the Google Tag (available at https://support.google.com/searchads/answer/7550511?hl=en); How Floodlight Recognizes Users (available at https://support.google.com/searchads/answer/2903014?hl=en); How Google Ads tracks website conversions (available at https://support.google.com/google-ads/answer/7521212); Google Ads Help, Cookie: Definition (available at https://support.google.com/google-ads/answer/2407785?hl=en); About demographic targeting in Google Ads (available at https://support.google.com/searchads/answer/7298581?hl=en&sjid=1196213575075458908-NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1); How Google Analytics Works (https://support.google.com/analytics/answer/12159447); Set up events (available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://support.google.com/analytics/answer/9267735).

[21] *See* Advertising (available at https://policies.google.com/technologies/ads?hl=en).

[22] *Id.*

[23] *Id.*



GET
200

https://googleads.g.doubleclick.net/pagead/viewthroughc
async=1&gtm=45He3b81v71692355&gcd=11l1l1l1l1&dma=0&u_w=
tps%3A%2F%2Fus.coca-cola.com%2Fproducts%2Fcoca-cola&hn=
id=163508170.1699914231&fledge=1&uaa=arm&uab=64&uafvl=G
0&uamb=0&uap=macOS&uapv=13.5.0&uaw=0&rfmt=3&fmt=4

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	googleads.g.doubleclick.net
:method	GET
:path	/pagead/viewthroughconversion/AW-10819297358/?random=1699914363626&cv=11&fst=1699914363626&bg=ffffff&guid=ON&async=1&gtm=45He3b81v71692355&gcd=11l1l1l1l1&dma=0&u_w=2240&u_h=1260&url=https%3A%2F%2Fus.coca-cola.com%2Fproducts%2Fcoca-cola%2Foriginal&ref=https%3A%2F%2Fus.coca-cola.com%2Fproducts%2Fcoca-cola&hn=www.googleadservices.com&frm=0&tiba=Coca-Cola%C2%AE%20Original%20%7C%20Coca-Cola%C2%AE&auid=163508170.1699914231&fledge=1&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B119.0.6045.123%7CChromium%3B119.0.6045.123%7CNot%253FA_Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.5.0&uaw=0&rfmt=3&fmt=4
:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
cookie	ar_debug=1; DSID=AC1gg-Q-4ws3kmro7WJQ99i2hvhOrtogajGxqGubqFov9yOak0kr0c6pyJImUgmId-9waj6Gt5Qa5wGXBEqVa3x-U331lTbIWmQjRNoRpRXEgsx2zYySoNjA-b0Nh8wDODjmKkNGhZfBZBv49ek0d5ynLNU1Aar2dEwGfvr5Megxn1KBdjlAJOO5mRtwUFgrOEgue771sRC4lqv4Hy_jcWR-Ul4P8rmfO0D1HwljxlEmm_c82M09i6Ey66ldno796wqOXn_-ZcEolMiQAr-QK_Oudl43u7-B_E1ClhiujaDvKqMeavuVmHw; IDE=AHWqTUnw23PgZgtWzj_ztpZCvKor8KfNWra1nJ5w1gsR8hq0JQZZs8olpl9cRO-7Ctw
Host	googleads.g.doubleclick.net
referer	https://us.coca-cola.com/
sec-ch-ua	"Google Chrome";v="119", "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
sec-fetch-dest	script
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
x-client-data	CJS2yQEIpbbJAQipncoBCMTnygEIlKHLAQiGoM0BCOjFzQEIusjNARj1yc0BGOuNpRc=

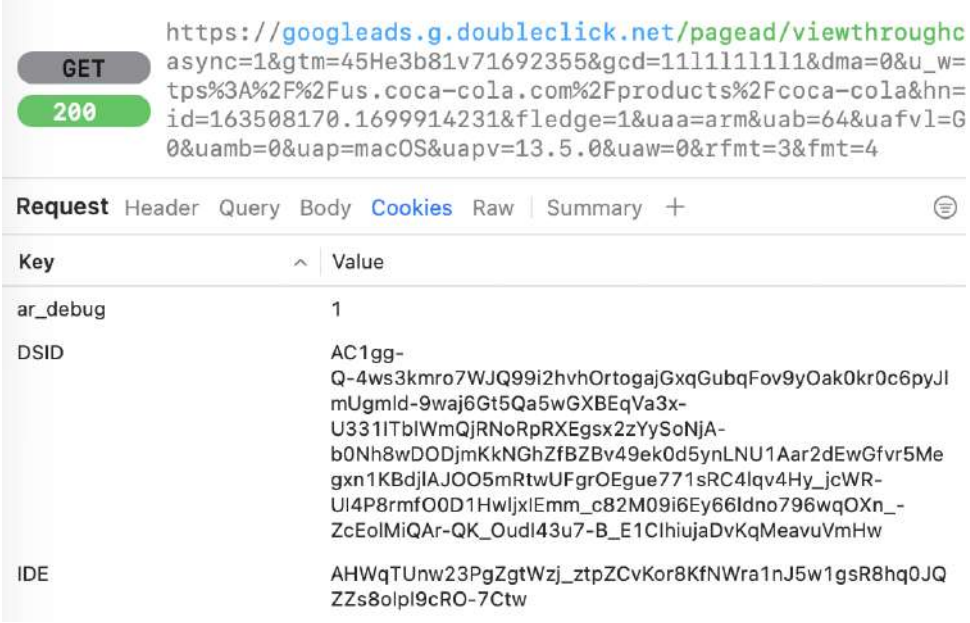


GET
200

https://googleads.g.doubleclick.net/pagead/viewthroughc
async=1&gtm=45He3b81v71692355&gcd=11l1l1l1l1&dma=0&u_w=
tps%3A%2F%2Fus.coca-cola.com%2Fproducts%2Fcoca-cola&hn=
id=163508170.1699914231&fledge=1&uaa=arm&uab=64&uafvl=G
0&uamb=0&uap=macOS&uapv=13.5.0&uaw=0&rfmt=3&fmt=4

Request Header Query Body Cookies Raw Summary +

Key	Value
async	1
auid	163508170.1699914231
bg	ffffff
cv	11
dma	0
fledge	1
fmt	4
frm	0
fst	1699914363626
gcd	11l1l1l1l1
gtm	45He3b81v71692355
guid	ON
hn	www.googleadservices.com
random	1699914363626
ref	https://us.coca-cola.com/products/coca-cola
rfmt	3
tiba	Coca-Cola® Original | Coca-Cola®
u_h	1260
u_w	2240
uaa	arm
uab	64
uafvl	Google%20Chrome;119.0.6045.123|Chromium;119.0.6045.123|Not%3FA_Brand;24.0.0.0
uamb	0
uap	macOS
uapv	13.5.0
uaw	0
url	https://us.coca-cola.com/products/coca-cola/original



[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

67. Data is also sent to Google when users browse the BODYARMOR Website. For example:



GET 200 https://googleads.g.doubleclick.net/pagead/id

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	googleads.g.doubleclick.net
:method	GET
:path	/pagead/id
:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
cookie	ar_debug=1; IDE=AHWqTUkmW_I00DfNdwA56znvaeSIQ9-TLmTO8msAJ29sabEkQJq0cskKdZj58bar; receive-cookie-deprecation=1
Host	googleads.g.doubleclick.net
origin	https://www.youtube.com
priority	u=1, i
referer	https://www.youtube.com/
sec-ch-ua	"Not A(Brand";v="99", "Google Chrome";v="121", "Chromium";v="121"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"Windows"
sec-fetch-dest	empty
sec-fetch-mode	cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
x-client-data	CJC2yQEIpLbJAQipncoBCKL1ygEIk6HLAQjwmM0BCIWgzQEIou7NAQjB7s0BCIPwzQEYp+rNARjJ+M0BGOuNpRc=

GET 200 https://googleads.g.doubleclick.net/pagead/id

Request Header Query Body Cookies Raw Summary +

Key	Value
ar_debug	1
IDE	AHWqTUkmW_I00DfNdwA56znvaeSIQ9-TLmTO8msAJ29sabEkQJq0cskKdZj58bar
receive-cookie-deprecation	1

68. Data is also sent to Google when users browse the Diet Coke Website. For example:

GET 200 https://googleads.g.doubleclick.net/pagead/id

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	googleads.g.doubleclick.net
:method	GET
:path	/pagead/id
:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
cookie	ar_debug=1; IDE=AHWqTUlEoVve9_SgQFNi8atpjJ1ZoN9jk3jWeRxkdXhmlHMLuj9eW_V0ovajY7GSAb0
Host	googleads.g.doubleclick.net
origin	https://www.youtube.com
priority	u=1, i
referer	https://www.youtube.com/
sec-ch-ua	"Not_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"Windows"
sec-fetch-dest	empty
sec-fetch-mode	cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
x-client-data	CJC2yQEIpLbJAQipncoBCKL1ygEIk6HLAQjwmM0BCIWgzQEIou7NAQjB7s0BCIPwzQEYp+rNARj68s0BGOuNpRc=

GET 200 https://googleads.g.doubleclick.net/pagead/id

Request Header Query Body Cookies Raw Summary +

Key	Value
ar_debug	1
IDE	AHWqTUlEoVve9_SgQFNi8atpjJ1ZoN9jk3jWeRxkdXhmlHMLuj9eW_V0ovajY7GSAb0

69. The "url" and "tiba" parameters disclose to Google the exact webpage and title that the user was viewing.

70. The "u_h" and "u_w" parameters correspond to the user's screen height and width.

71. Google documentation confirms that the "IDE" cookie is used for advertising. Specifically, it is "used to show Google ads on non-Google sites."[24]

72. Further, as shown above, along with all of this data, the Google software code that Defendant causes to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to Google.

73. As discussed above, the "user-agent" corresponds to the device and browser that the user has used to access the Websites.

74. Finally, the data sent to Google contains the user's IP address.

75. Because Google's cookies operate across multiple sites (i.e., cross-site tracking), the cookies enable Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google states that when users visit sites or apps using Google's ad or analytics services, "those services may link information about your activity from that site or app with activity from other sites or apps that use our services."[25] Google's advertising platform aggregates user data to create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics and audience segments based on shared traits (such as females, Millennials, etc.), and to perform targeted advertising and marketing analytics.

76. Google's consumer profiles span across the user's devices and across households.[26] Google states that it "may infer whether activity from different devices, browsing sessions, or accounts is associated," and links mobile advertising IDs to advertising cookies "to coordinate ads across [users'] mobile apps and mobile browser."[27] Users may then receive ads

[24] https://policies.google.com/technologies/cookies?hl=en-US.
[25] *See* Why Google collects data (available at https://policies.google.com/privacy?fg=1&hl=en-GB).
[26] *See* Advertising (available at https://policies.google.com/technologies/ads?hl=en).
[27] *Id.*

on household connected TVs related to the web or app activity from devices within their household.[28]

77. Thus, the Google cookies used on the Websites enable Google to track users' interactions with advertisements to help advertisers understand how users engage with ads across different websites. Further, the user data collected through the cookie enables the delivery of personalized ads based on user interests and behaviors. For instance, if a user frequently visits travel-related websites, Google will show that user more travel-related advertisements. The collected data is also used to generate reports for advertisers, helping them assess the performance of their ad campaigns and make data-driven decisions (such as renaming their products). Google's advertising platform also enables advertisers to retarget marketing, which Google explains allows advertisers to "show previous visitors ads based on products or services they viewed on your website. With messages tailored to your audience, dynamic remarketing helps you build leads and sales by bringing previous visitors back to your website to complete what they started."[29]

78. Further, in its "Shared Data Under Measurement Controller-Controller Data Protection Terms," Google states: "Google can access and analyze the Analytics data customers share with us to better understand online behavior and trends, and improve our products and services—for example, to improve Google search results, detect and remove invalid advertising traffic in Google Ads, and test algorithms and build models that power services like Google Analytics Intelligence that apply machine-learning to surface suggestions and insights for customers based on their analytics data and like Google Ads that applies broad models to improve ads personalization and relevance. These capabilities are critical to the value of the products we deliver to customers today."[30] Thus, Google has the capability to use the data it collects for understanding online behavior and trends, machine learning, and improving its own products and services.

---

[28] *Id.*

[29] Dynamic remarketing for web setup guide (available at https://support.google.com/google-ads/answer/6077124).

[30] Shared Data Under Measurement Controller-Controller Data Protection Terms (available at https://support.google.com/analytics/answer/9024351).

3. TikTok Cookies (Coca-Cola, Vitaminwater, Sprite, Fanta, and Smartwater Websites).

79. Defendant also causes third-party cookies to be transmitted between the Websites' users' browsers and devices and the **analytics.tiktok.com** domain, even after users adjust the available toggle switches to decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies (except those "Necessary Cookies" needed for the Websites to function). This domain is associated with TikTok for Business, a suite of tools offered by TikTok USDS Joint Venture LLC. The TikTok social media platform is used to create and share short-form videos, and it utilizes cookies for various purposes including assisting brands and marketers to create, manage, and optimize ad campaigns on the platform.[31]

80. TikTok utilizes cookies to collect data on user interactions with websites that have integrated TikTok's tracking technologies (such as the Websites). These cookies are used to "measure and improve the performance of your advertising campaigns and to personalize the user's experience (including ads) on TikTok."[32] TikTok further explains that it uses cookies to "match events with people who engage with your content on TikTok. Matched events are used to improve measurement and optimize ad campaigns. They can also contribute to building your retargeting and engagement audiences." *Id.* These cookies enable TikTok to recognize and track users across different sessions and domains (i.e., cross-site tracking) and to collect and synchronize user data to observe and evaluate TikTok user behavior.

81. These cookies enable TikTok to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, including

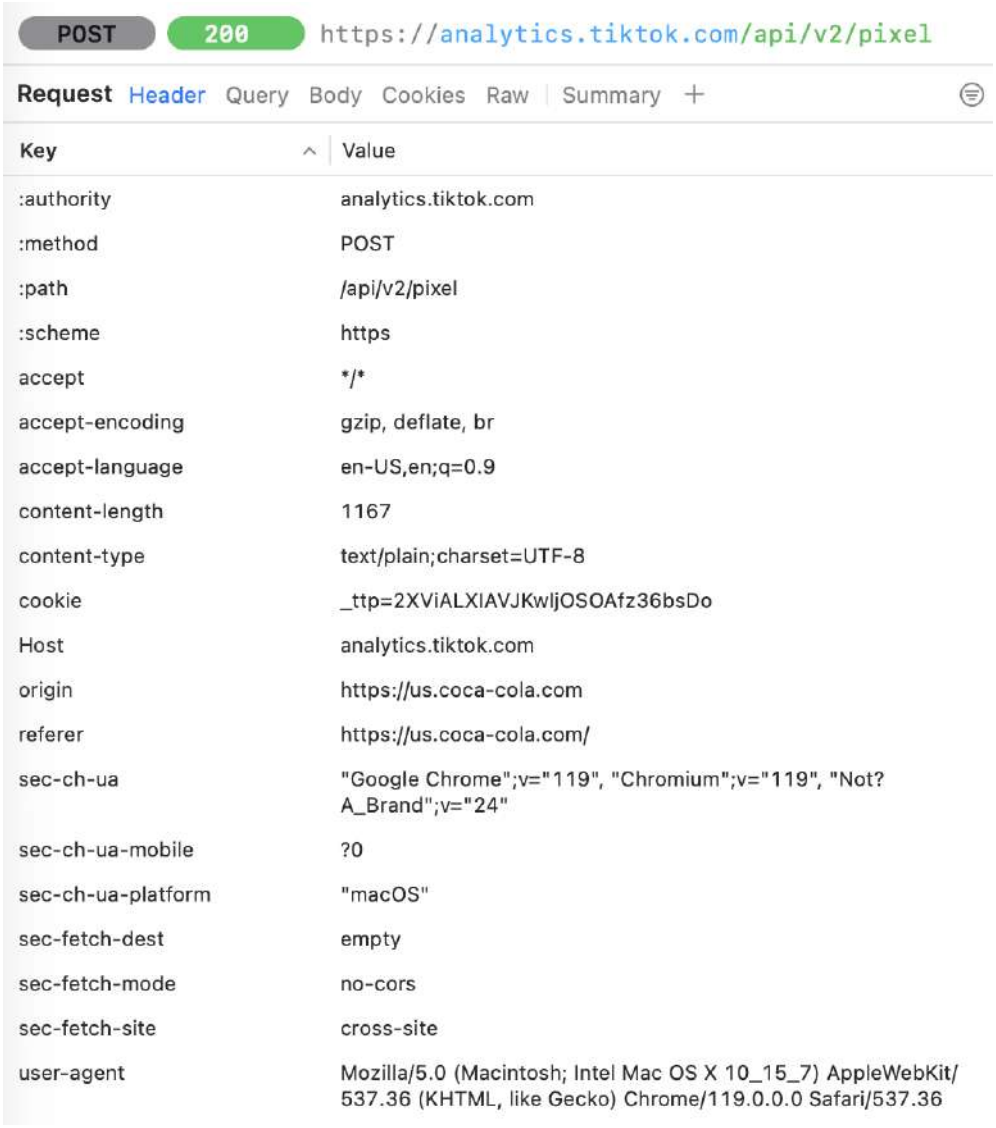
[31] *See, e.g.*, TikTok for Business (https://ads.tiktok.com/business/en-US/products/ads; and https://ads.tiktok.com/business/en-US/products/measurement); TikTok Business Help Center; Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).

[32] TikTok Business Help Center; Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).

email addresses and phone numbers, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) session information, (x) user identifiers, and (xi) geolocation data in the form of the IP address.[33]

82. For example, the TikTok software code that Defendant causes to be stored on and executed by the Website user's device causes the following data to be sent to TikTok's domain, at analytics.tiktok.com, when the user browses the Coca-Cola Website, even after the user has rejected all Advertising, Analytics, and Personalization cookies:

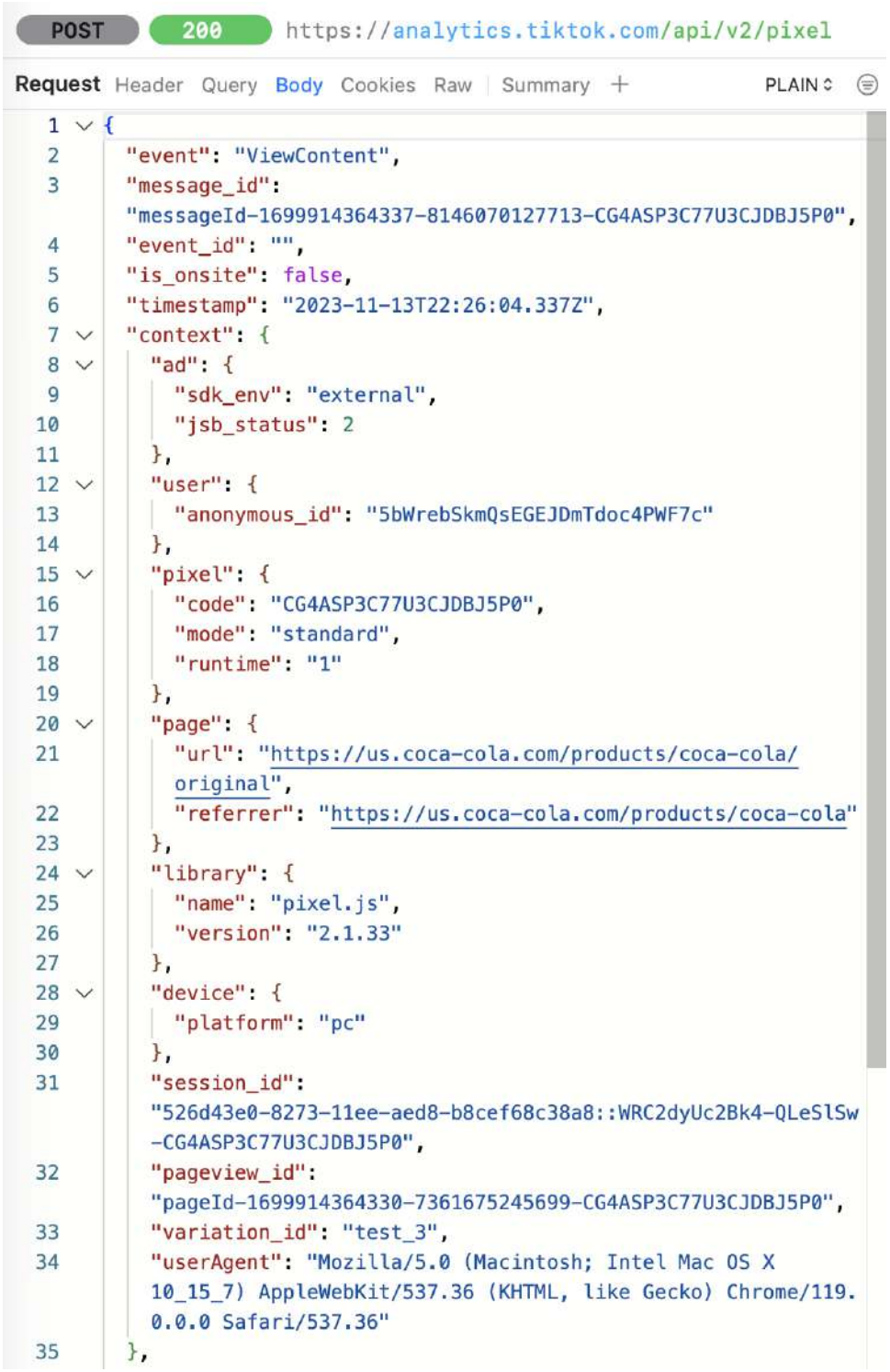
[33] *Id.*; *see also* TikTok for Business: Enhance Data Postback with the TikTok Pixel (https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel?lang=en); TikTok for Business: Advanced Matching for Web (available at https://ads.tiktok.com/help/article/advanced-matching-web?redirected=1); TikTok for Business: About TikTok Pixel (available at https://ads.tiktok.com/help/article/tiktok-pixel?lang=en).



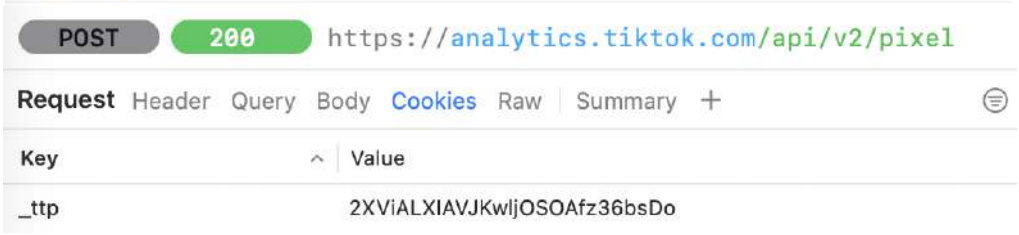
POST 200 https://analytics.tiktok.com/api/v2/pixel

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	analytics.tiktok.com
:method	POST
:path	/api/v2/pixel
:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
content-length	1167
content-type	text/plain;charset=UTF-8
cookie	_ttp=2XViALXIAVJKwljOSOAfz36bsDo
Host	analytics.tiktok.com
origin	https://us.coca-cola.com
referer	https://us.coca-cola.com/
sec-ch-ua	"Google Chrome";v="119", "Chromium";v="119", "Not? A_Brand";v="24"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
sec-fetch-dest	empty
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36

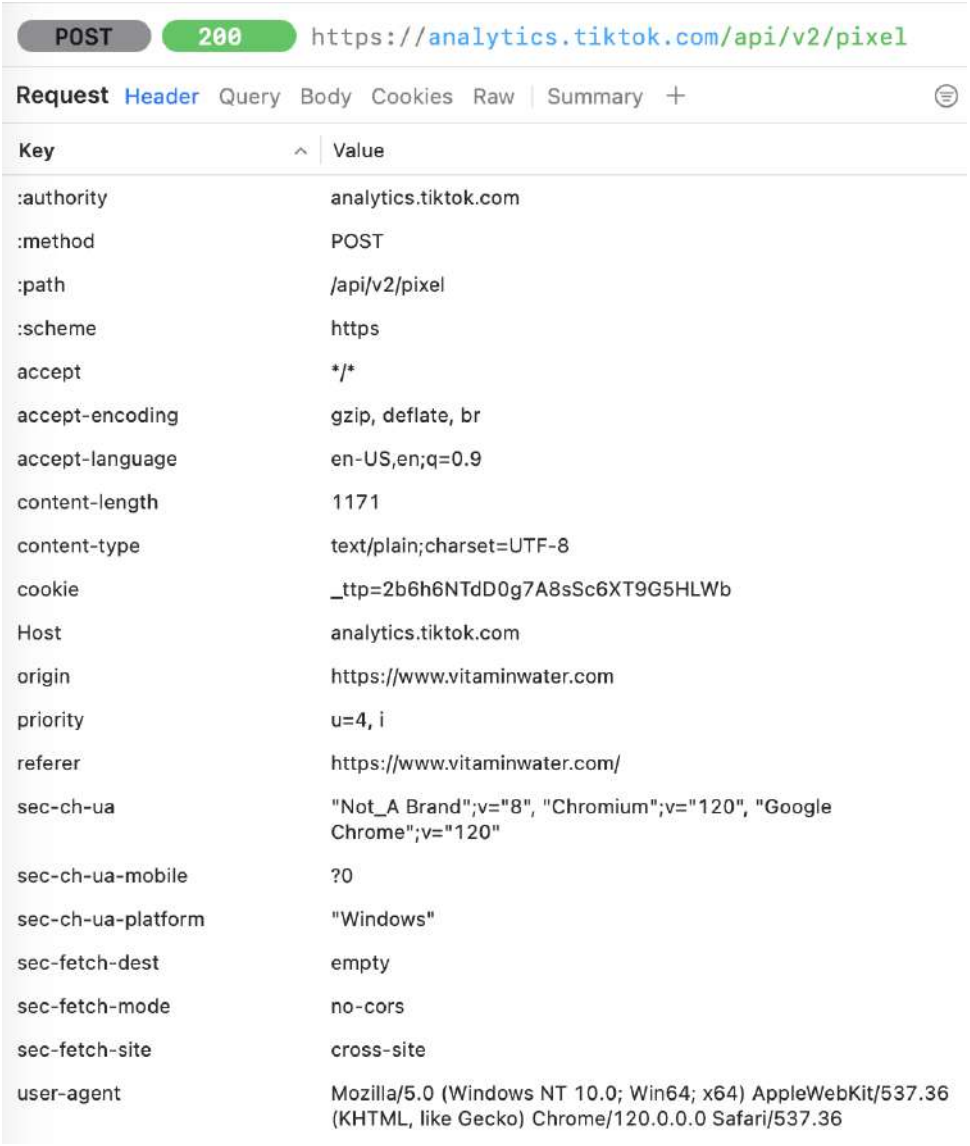

POST
200
https://analytics.tiktok.com/api/v2/pixel
Request Header Query Body Cookies Raw Summary
PLAIN
{
"event": "ViewContent",
"message_id": "messageId-1699914364337-8146070127713-CG4ASP3C77U3CJDBJ5P0",
"event_id": "",
"is_onsite": false,
"timestamp": "2023-11-13T22:26:04.337Z",
"context": {
"ad": {
"sdk_env": "external",
"jsb_status": 2
},
"user": {
"anonymous_id": "5bWrebSkmQsEGEJDmTdoc4PWF7c"
},
"pixel": {
"code": "CG4ASP3C77U3CJDBJ5P0",
"mode": "standard",
"runtime": "1"
},
"page": {
"url": "https://us.coca-cola.com/products/coca-cola/original",
"referrer": "https://us.coca-cola.com/products/coca-cola"
},
"library": {
"name": "pixel.js",
"version": "2.1.33"
},
"device": {
"platform": "pc"
},
"session_id": "526d43e0-8273-11ee-aed8-b8cef68c38a8::WRC2dyUc2Bk4-QLeSlSw-CG4ASP3C77U3CJDBJ5P0",
"pageview_id": "pageId-1699914364330-7361675245699-CG4ASP3C77U3CJDBJ5P0",
"variation_id": "test_3",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36"
},

```
  "_inspection": {},
  "signal_diagnostic_labels": {
    "raw_email": {
      "label": "missing"
    },
    "raw_auto_email": {
      "label": "missing"
    },
    "raw_phone": {
      "label": "missing"
    },
    "raw_auto_phone": {
      "label": "missing"
    },
    "hashed_email": {
      "label": "missing"
    },
    "hashed_phone": {
      "label": "missing"
    }
  },
  "properties": {
    "is_standard_mode": "1"
  }
}
```

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

83. Similarly, the following types of data and cookies are sent to TikTok when a user browses the Vitaminwater Website:



POST 200 https://analytics.tiktok.com/api/v2/pixel

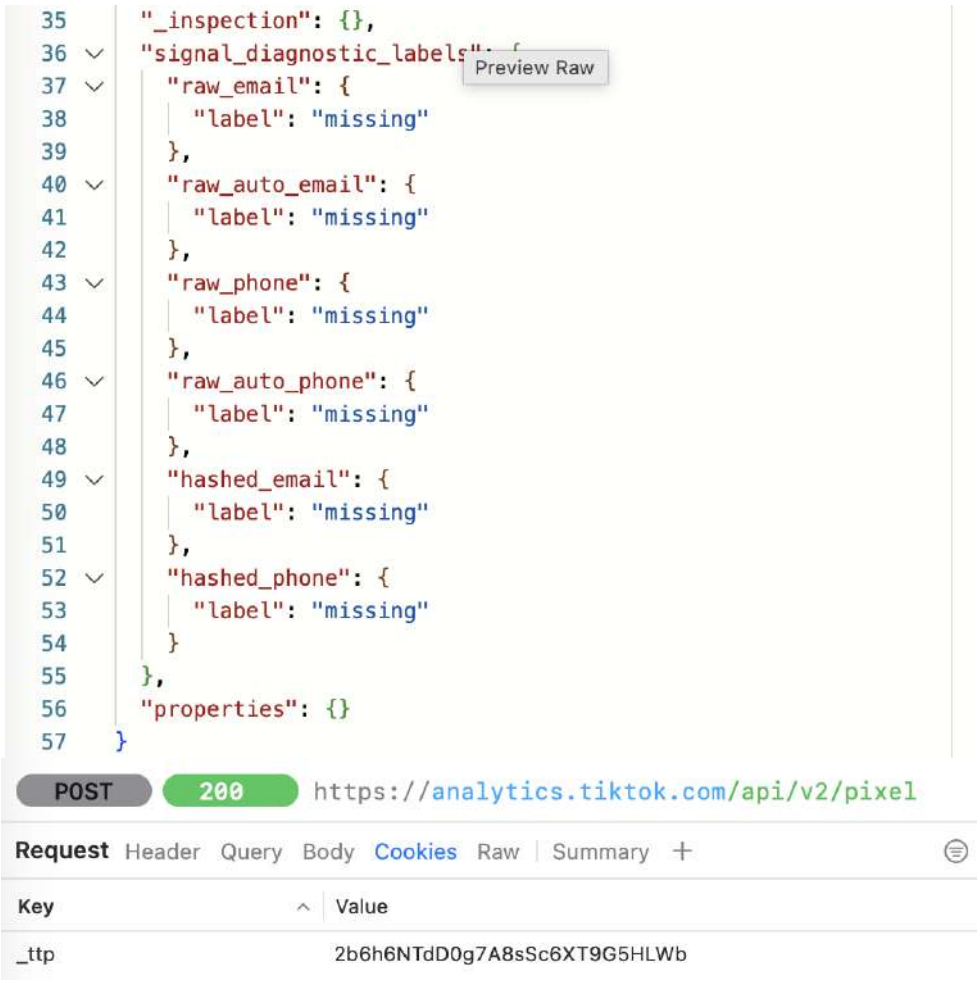
Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	analytics.tiktok.com
:method	POST
:path	/api/v2/pixel
:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
content-length	1171
content-type	text/plain;charset=UTF-8
cookie	_ttp=2b6h6NTdD0g7A8sSc6XT9G5HLWb
Host	analytics.tiktok.com
origin	https://www.vitaminwater.com
priority	u=4, i
referer	https://www.vitaminwater.com/
sec-ch-ua	"Not_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"Windows"
sec-fetch-dest	empty
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

POST 200 https://analytics.tiktok.com/api/v2/pixel

Request Header Query Body Cookies Raw Summary + PLAIN


```
{
  "event": "Pageview",
  "message_id":
  "messageId-1705541431281-6454253190575-CG0H3P3C77U3CJDBDJS0",
  "event_id": "",
  "is_onsite": false,
  "timestamp": "2024-01-18T01:30:31.281Z",
  "context": {
    "ad": {
      "sdk_env": "external",
      "jsb_status": 2
    },
    "user": {
      "anonymous_id": "sa_rdlHVDNFzK-yfV837AP-CHFW"
    },
    "pixel": {
      "code": "CG0H3P3C77U3CJDBDJS0",
      "runtime": "1"
    },
    "page": {
      "url": "https://www.vitaminwater.com/products/
      vitaminwater-zero-sugar/shine-strawberry-lemonade",
      "referrer": "https://www.vitaminwater.com/products/
      vitaminwater-zero-sugar"
    },
    "library": {
      "name": "pixel.js",
      "version": "2.1.33"
    },
    "device": {
      "platform": "pc"
    },
    "session_id":
    "c47aeb18-b5a0-11ee-b70a-08c0eb5e39ec::_sXdi6xBcOX-oJqhWm9Z
    -CG0H3P3C77U3CJDBDJS0",
    "pageview_id":
    "pageId-1705541431267-9958861968947-CG0H3P3C77U3CJDBDJS0",
    "variation_id": "test_3",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
    Safari/537.36"
  },
```



[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

84. Similarly, the following type of data and cookies are sent to TikTok when a user browses the Sprite Website:

POST 200 https://analytics.tiktok.com/api/v2/pixel

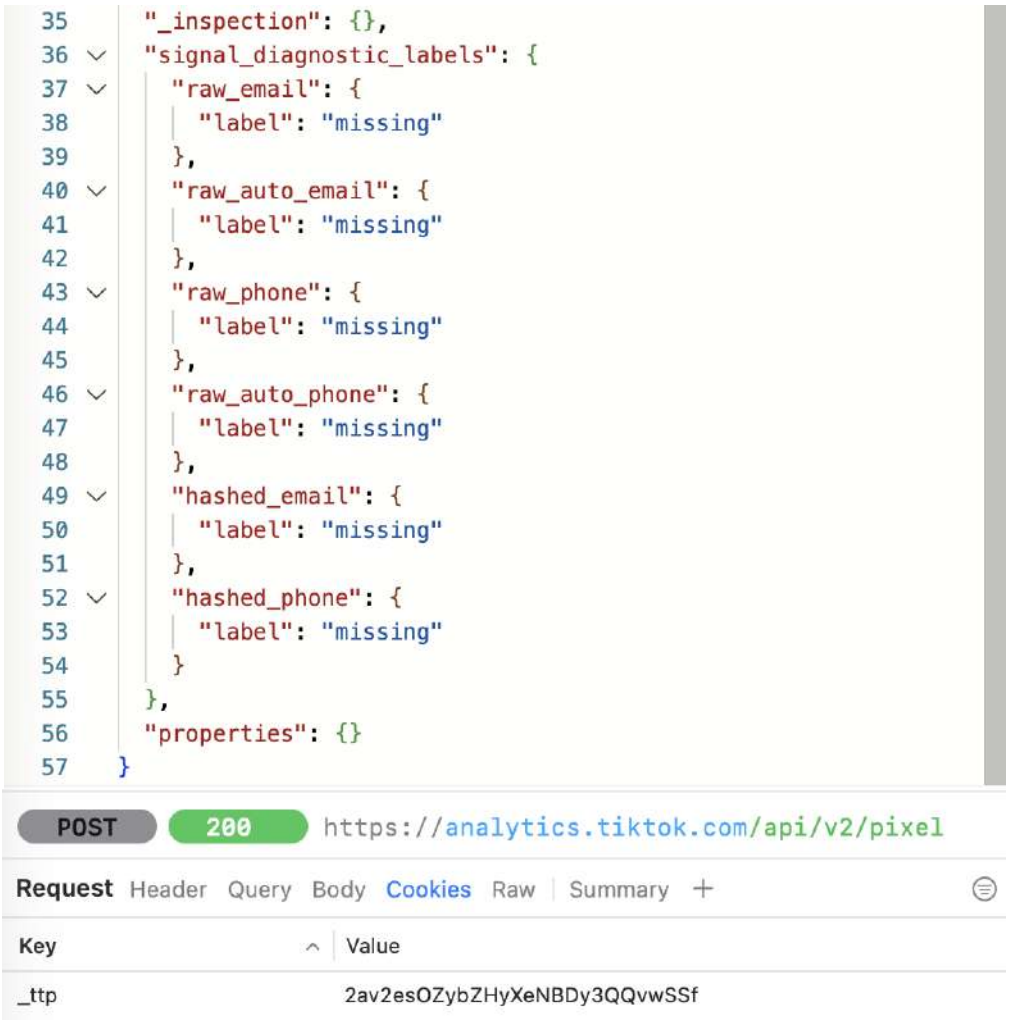
Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	analytics.tiktok.com
:method	POST
:path	/api/v2/pixel
:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.9
content-length	1099
content-type	text/plain;charset=UTF-8
cookie	_ttp=2av2esOZybZHyXeNBDy3QQvwSSf
Host	analytics.tiktok.com
origin	https://www.sprite.com
priority	u=4, i
referer	https://www.sprite.com/
sec-ch-ua	"Not_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"Windows"
sec-fetch-dest	empty
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

POST 200 https://analytics.tiktok.com/api/v2/pixel

Request Header Query Body Cookies Raw Summary + PLAIN


```
{
  "event": "Pageview",
  "message_id":
  "messageId-1705538259810-4773988752111-CG0GVIRC77UAN2JP4GT0",
  "event_id": "",
  "is_onsite": false,
  "timestamp": "2024-01-18T00:37:39.810Z",
  "context": {
    "ad": {
      "sdk_env": "external",
      "jsb_status": 2
    },
    "user": {
      "anonymous_id": "qjx0GAEkHiAeO9v1j3yxmA-vC7R"
    },
    "pixel": {
      "code": "CG0GVIRC77UAN2JP4GT0",
      "runtime": "1"
    },
    "page": {
      "url": "https://www.sprite.com/products/sprite-cherry",
      "referrer": "https://www.sprite.com/products"
    },
    "library": {
      "name": "pixel.js",
      "version": "2.1.33"
    },
    "device": {
      "platform": "pc"
    },
    "session_id":
    "9702e52a-b599-11ee-9f6d-0010e0e4d010::qTWBiTpLnBSEL2abd2Jz
    -CG0GVIRC77UAN2JP4GT0",
    "pageview_id":
    "pageId-1705538259801-2230430669164-CG0GVIRC77UAN2JP4GT0",
    "variation_id": "test_3",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0
    Safari/537.36"
  },
```



85. The data includes the "session_id," which is a unique identifier generated by TikTok to track a user's activity. This allows TikTok to correlate the user's behavior from a browsing session, including page views and conversions, to a particular user to enhance advertising measurement, attribution, and targeting.[34]

86. The data further indicates, among other things, the exact URLs that the user was visiting on the Website in question.

87. The data further includes the "_ttp" cookie. According to TikTok's documentation, the "_ttp" cookie is one of the company's advertising cookies, the purpose of which is "[t]o measure and improve the performance of your advertising campaigns and to

[34] *See, e.g.*, How to get TikTok session id? (available at https://gbtimes.com/how-to-get-tiktok-session-id/).

personalize the user's experience (including ads) on TikTok."[35] The "_ttp" cookie is created and owned by TikTok on TikTok's server and is used to recognize and match events across different websites, is enabled by default, and lasts 13 months from the last date it was used.[36]

88. Further, along with all of this data, the TikTok software code that Defendant causes to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to TikTok.

89. As discussed above, the "user-agent" corresponds to the device and browser that the user has used to access the Websites.

90. Finally, the data sent to TikTok includes the user's IP address.

91. The other Websites that send cookie data to TikTok even after users have rejected all unnecessary cookies (i.e., the Fanta and Smartwater Websites) operate in substantially the same way as the Websites described above, with each of those Websites sending substantially the same type of header data, body data, and cookie data to TikTok even after users have rejected all unnecessary cookies.

92. By collecting this user data, TikTok performs user behavior tracking (i.e., monitoring user actions like page views, clicks, and interactions to understand user engagement); advertising optimization (i.e., gathering data to enhance the relevance and effectiveness of TikTok advertising campaigns); and performance measurement (i.e., assessing the success of marketing efforts by analyzing user responses to ads and content).[37]

93. Further, TikTok's marketing materials provide that its Automatic Advanced Matching feature allows advertisers to use cookies to "[m]atch your website visitors with people on TikTok, to expand audience sizes for solutions like web retargeting."[38] TikTok's Automatic Advanced Matching feature functions as follows: "When a visitor lands on your website and inputs customer information during registration, sign-in, contact, or checkout on a website where

---

[35] *See* TikTok for Business: Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).
[36] TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel).
[37] *See* TikTok for Business: Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).
[38] TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel).

you installed your pixel, Automatic Advanced Matching will capture information from those fields. … TikTok will use hashed information to link event information to people on TikTok. TikTok may use matched events to better attribute events to TikTok ads, optimize advertisers' future campaigns, and depending on advertisers' and users' settings, TikTok may also add people to advertisers' retargeting or engagement audiences."[39]

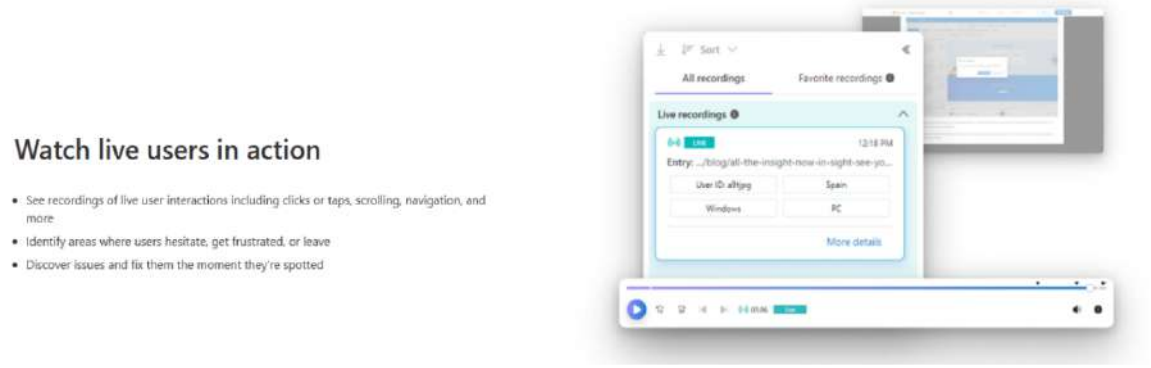
4. Microsoft Clarity Cookies (the Fairlife Website).

94. Defendant also causes third-party cookies to be transmitted between the Websites' users' browsers and devices and the **clarity.ms** domain, even after users adjust the available toggle switches to decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies (except those "Necessary Cookies" needed for the Websites to function). This domain is associated with Clarity, Microsoft's "cutting-edge behavioral analytics tool that helps you understand user interaction with your website or app".[40] Clarity is a Microsoft Advertising tool, which is "crucial for successful marketing."[41] "Clarity's tracking code … uses a cookie to obtain user session data." [42]

95. Clarity allows Defendant to "watch live users in action" via "recordings of live user interactions" on the website, including a user's "clicks or taps, scrolling, navigation, and more."[43] Indeed, Clarity boasts that it "tracks all visitor clicks and scrolls on mobile, desktop, and tablet[.]" These "session recordings" track each and every consumer's individual actions on the website.[44]

---

[39] TikTok for Business: How to set up Automatic Advanced Matching (available at https://ads.tiktok.com/help/article/how-to-set-up-automatic-advanced-matching?lang=en).
[40] https://learn.microsoft.com/en-us/clarity/setup-and-installation/about-clarity.
[41] https://about.ads.microsoft.com/en/blog/post/october-2021/introducing-microsoft-clarity-insights-for-microsoft-advertising.
[42] https://learn.microsoft.com/en-us/clarity/setup-and-installation/cookie-consent.
[43] https://clarity.microsoft.com/session-recordings.
[44] *Id*.



96. Further, Clarity permits Defendant to aggregate individual users' session recordings into "heatmaps" for Defendant's financial gain. Heatmaps are "visualization tool[s]" aimed at "aggregat[ing] information about how users interact with the website." [45] This allows Defendant to "[s]ee at a glance which areas on [web site owner's] page drive the most engagement," a crucial element to increasing advertising revenue. [46] Clarity also permits Defendant to "track a specific subset of users," including tracking metrics like what browser users visited from, what type of device, the date, and more. Clarity even permits the use of specific "Clarity user ID[s]" which permits Clarity to track users across their devices, and identify when the same user visits the website multiple times.[47] Businesses use Clarity to "make data-driven decisions" to "improve overall conversion rates" of clicks, engagement, or sales.[48] Microsoft notes in a Clarity case study that Clarity cookies permitted businesses to see a "substantial increase" in "purchases." [49] In one instance, "following just five days after implementing Clarity, the [business] saw an uplift of 19% in conversion rate."[50] Businesses

[45] https://learn.microsoft.com/en-us/clarity/heatmaps/heatmaps-overview.
[46] https://clarity.microsoft.com/heatmaps.
[47] https://clarity.microsoft.com/insights; https://learn.microsoft.com/en-us/clarity/setup-and-installation/identify-api.
[48] https://clarity.microsoft.com/case-studies/ecommerce-boost/#:~:text=Using%20Clarity&text=By%20analyzing%20user%20sessions%20and,and%20improve%20overall%20conversion%20rates.
[49] *Id.*
[50] *Id.*

consider Clarity a "must-have tool for any business serious about optimizing their website and increasing online revenue."[51]

97. Microsoft collects data from Clarity,[52] which "Microsoft retains . . . for as long as necessary[.]"[53] Clarity cookies allow Microsoft to obtain and store at least the following user data: (i) user identifier; (ii) website interactions (such as user data input into websites and the contents of pages viewed); (iii) interests and preferences; (iv) shopping behavior; (v) device information; (vi) demographic data; (vii) geolocation data; (viii) referring URL; and (ix) session information. [54] Microsoft states that it may use the user data it collects to develop and train its AI models.[55]

5. Snapchat Cookies (Coca-Cola, Fanta, Sprite, Powerade, Diet Coke, Vitaminwater, Fairlife, Simply, and Smartwater Websites).

98. Defendant also causes third-party cookies to be transmitted between the Websites' users' browsers and devices and the **tr.snapchat.com** domain, even after users adjust the available toggle switches to decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies (except those "Necessary Cookies" needed for the Websites to function). This domain is associated with Snap Inc., the social media company that owns Snapchat. Snapchat is a multimedia messaging app that lets users share photos, videos, text, and drawings—often designed to disappear after being viewed. Snap uses "sc_at" cookies as part of and in conjunction with identifying data and data on users' browsing history, choices, and interactions with advertisements.[56] This data helps Snap personalize ad content and track users across the internet.[57] As Snap explains, it uses the data

---

[51] https://clarity.microsoft.com/case-studies/ecommerce-boost/#:~:text=Using%20Clarity&text=By%20analyzing%20user%20sessions%20and,and%20improve%20overall%20conversion%20rates.
[52] https://www.microsoft.com/en-us/privacy/privacystatement.
[53] *Id*.
[54] https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-data.
[55] Microsoft Privacy Statement (available at https://www.microsoft.com/en-us/privacy/privacystatement).
[56] https://snapdiscoveries.com/what-is-tr-snapchat-com-is-used-for; *see also* Snapchat Business Help Center: Directly Implement the Pixel On Your Website (available at https://businesshelp.snapchat.com/s/article/pixel-direct-implementation).
[57] *Id*.

collected by Snapchat cookies "for optimization, custom audience creation, look-alike modeling, reporting, machine learning, and targeting capabilities. All uses are … meant to deliver better results for our ad products."[58]

99. Snapchat cookies allow Snap to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) demographic information, including age and location,[59] (v) user input data, including name and email address,[60] (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and/or (xii) geolocation data—including whether a user is located in California.

6. Additional Third-Party Cookies.

100. Defendant also causes third-party cookies to be transmitted between the Websites' users' browsers and devices and other domains, even after users adjust the available toggle switches to decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies (except those "Necessary Cookies" needed for the Websites to function), including: (i) adsrvr.org on the Coca-Cola, Sprite, Gold Peak, and Vitaminwater Websites; (ii) pinterest.com on the Coca-Cola, Gold Peak, Fairlife, Simply, and Smartwater Websites; (iii) analytics.twitter.com on the Topo Chico, BODYARMOR, and Smartwater Websites, and (iv) simage2.pubmatic.com on the Vitaminwater Website.

101. The **insight.adsrvr.org** and **js.adsrvr.org** domains are associated with The Trade Desk, Inc., a digital advertising company that offers a cloud-based ad-buying platform that enables businesses to plan, manage, optimize, and measure data-driven digital advertising campaigns.[61] The Trade Desk uses insight.adsrvr.org and js.adsrvr.org cookies to collect data on

---

[58] Snapchat Business Help Center: Pixel Implementation FAQ (available at https://businesshelp.snapchat.com/s/article/snap-pixel-faq); *see also* Snapchat Business Help Center: About Snap Pixel (available at https://businesshelp.snapchat.com/s/article/snap-pixel-about).

[59] *See* Snap for Developers: Parameters (available at https://developers.snap.com/api/marketing-api/Conversions-API/Parameters).

[60] *Id.*

[61] *See* The Trade Desk, Inc. 2023 Form 10-K (filed Feb. 15, 2024).

users such as their geographic locations, the type of device users are using, and users' interests as inferred from their web browsing or app usage activity.[62] This data helps The Trade Desk personalize ad content and track users across the internet.[63]

102. The Trade Desk acknowledges that its cookies' ability "to collect, augment, analyze, use and share data relies upon the ability to uniquely identify devices across websites and applications, and to collect data about user interactions with those devices for purposes such as serving relevant ads and measuring the effectiveness of ads."[64]

103. The **ct.pinterest.com** domain is associated with Pinterest, Inc., which operates a popular social media platform that allows users to discover, save, and share ideas as pins in the form of photos and videos. Businesses can upload and showcase their products through "Shop the Look" pins or Product Pins that directly link to e-commerce websites. Businesses install the Pinterest tag on their websites to track ad conversions. As Pinterest explains, "The Pinterest tag is a piece of code that you add to your website. It lets Pinterest track visitors to your site, as well as the actions they take on your site after seeing your Pinterest ad. This means you can measure how effective your Pinterest ads are by understanding the actions people take on your website after seeing or engaging with your ad."[65] Pinterest cookies can be used to identify and track people who purchase products, add items to a shopping cart, visit specific pages on the website, and/or search for specific items on the website.[66]

104. The **twitter.com** domain and its subdomains are associated with X Corp. (formerly Twitter) ('X'). X's cookies collect a wide range of user data, including a user's browsing history; IP address; interactions with advertisements; data used to authenticate and secure personal accounts; and data read from a device's local storage.[67] X uses the collected user

---

[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] Pinterest Help Center: Install the Pinterest Tag (available at https://help.pinterest.com/en/business/article/install-the-pinterest-tag).
[66] *See, e.g.*, Pinterest Help Center: Add event codes (available at https://help.pinterest.com/en/business/article/add-event-codes); Pinterest Help Center: View tag parameters and cookies (available at https://help.pinterest.com/en/business/article/pinterest-tag-parameters-and-cookies).
[67] *See* https://help.x.com/en/rules-and-policies/x-cookies.

data to target users with personalized advertisements and content, generate analytics on website interaction, and conduct unspecified "Research and Development."[68]

105. For example, the X code that the Website causes to be executed by the user's browser causes the browser to send the following types of cookies and other data to X:



[68] *Id.*



106. The cookie and the other data enable X to track the user (or "guest") across various X-integrated websites, in order to target advertisements to the user. According to X documentation, for example, the "personalization_id" cookie "tracks activities on and off Twitter

for a personalized experience."[69] The "guest_id_marketing" and "guest_id_ads" cookies are "for advertising when logged out."[70]

107. X states that "[w]hen [users] view X content such as embedded posts, buttons, or timelines integrated into other websites using X for Websites, X may receive information including the web page [the user] visited, [their] IP address, browser type, operating system, and cookie information. This information helps us to improve our products and services."[71]

108. The **pubmatic.com** domain (including **simage2.pubmatic.com**) is associated with PubMatic, Inc., a digital advertising company. PubMatic uses pubmatic.com cookies to collect data on user behavior on websites including user interactions with advertising content.[72] PubMatic uses this data to personalize advertising content and track users across the internet.[73]

109. The Trade Desk, Pinterest, X, and PubMatic cookies allow those Third Parties to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) demographic information, (v) interests and preferences, (vi) shopping behaviors, (vii) device information, (viii) referring URLs, (ix) session information, (x) user identifiers, and/or (xi) geolocation data—including whether a user is located in California.

D. The Third Parties Intercept User Communications While in Transit.

110. On information and belief, the Third Parties intercept user communications while those communications are in transit between the user's browsers and Defendant's Websites. The Third Parties operate large-scale data ingestion systems designed to receive, read, and act upon incoming data streams in real time, as the data is transmitted over the network, before it is committed to storage. As the user data is transmitted over the wire, it is transmitted as a raw payload that cannot be used until the Third Party reads and processes it using at least the steps described below. These steps necessarily require contemporaneous access to the contents of the communications while they are in transit.

---

[69] How cookies are used on X (available at https://help.x.com/en/rules-and-policies/x-cookies).
[70] *Id.*
[71] X for Websites (available at https://help.x.com/en/x-for-websites-ads-info-and-privacy).
[72] *See* PubMatic, Inc. Form 10-K for year ending December 31, 2023 (Filed Feb. 28, 2024) at 17–18.
[73] *Id.*

111. First, the Third Parties must read the data in real time in order to ***transform*** it into a usable format for subsequent processing. Transforming, for example, may involve decoding long HTML-encoded strings into a format such as Unicode Transformation Format, which is more amenable to subsequent processing.

112. Second, the Third Parties read the data in real time in order to ***deduplicate*** events transmitted through multiple channels. Many websites transmit the same user interaction twice: both directly from the user's device and separately through a server-to-server API, to ensure reliability.[74] Third Party platforms encourage this redundant configuration and automatically compare identifiers contained within the transmitted data—such as event identifiers and device identifiers—to determine whether multiple transmissions correspond to the same user action.[75] This deduplication occurs as the communications are received, before they are stored.

113. Third, the Third Parties read and analyze incoming communications in real time to ***validate*** and ***filter*** the data, including to detect invalid, malicious, or anomalous transmissions and to determine whether the data complies with internal processing rules. These determinations must be made immediately upon receipt of the communication in order for the Third Parties' systems to function.

114. Fourth, the Third Parties perform real-time ***analytics*** on user communications to determine their meaning and significance. This processing is used to interpret the data, to associate it with particular users or devices, and to determine what real-time events or actions should be taken in response, such as triggering advertising delivery, notifications, or other automated responses. This step typically involves applying artificial intelligence and machine

---

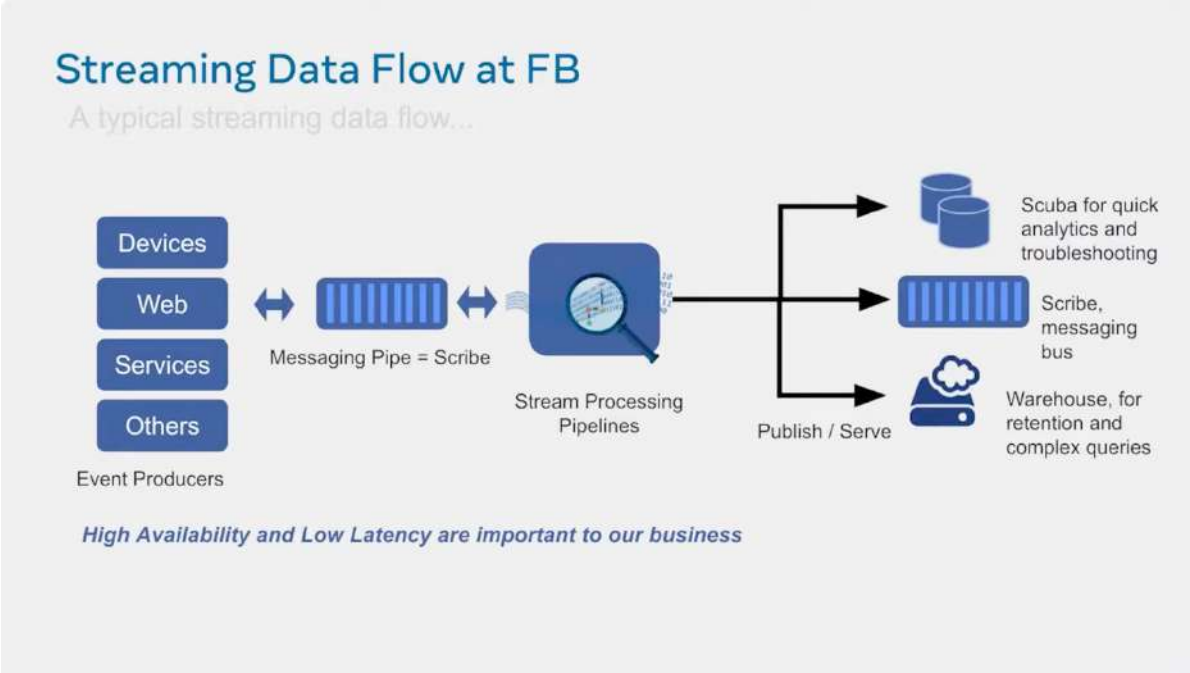
[74] For example, Google's server-to-server API is the **Google Ads Conversion API**. Facebook's is the **Meta Conversions API**. TikTok uses the **TikTok Events API**. Snapchat's is the **Snapchat Conversions API**. Pinterest's uses the **Pinterest Conversions API**. On information and belief, each of the Third Parties uses a server-to-server API to collect user data.

[75] For example, Facebook recommends that websites use a "redundant setup" whereby "advertisers implement the Conversions API alongside their Meta Pixel." *See* "Handling Duplicate Pixel and Conversions API Events," available at https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events. Facebook confirms that its system automatically deduplicates events using various parameters included with the data, such as "event_id," "event_name," "fbp," and "external_id." *Id.*

learning algorithms to the data. These determinations occur while the data is in motion, prior to final storage.

115. To accomplish each of the functions described above, the Third Parties employ real-time stream processing platforms specifically designed to operate on data "in flight"—that is, after it is transmitted from a user's browser but before it is committed to the Third Parties' storage. Examples of such platforms include Apache Flink, Kafka, and Amazon Kinesis. Industry documentation confirms that these systems are designed to read, transform, analyze, and act upon data streams as they are received.

116. For example, Meta (formerly Facebook) has publicly described its proprietary real-time stream processing platform that ingests data transmitted from users' devices and websites, applies real-time transformations and personalization, and only thereafter stores the data in backend data warehouses, as illustrated in the following diagram created by Meta:[76]



117. As the diagram confirms, the data is sent from consumers' "Devices" and from the "Web," and then goes through the Stream Processing Pipelines ***before*** being stored in the data "Warehouse."

---

[76] XStream: Stream Processing Platform at Facebook (video) at 1:07 (available at https://www.youtube.com/watch?v=DNI54vc1ALQ).

118. Meta's Stream Processing Pipelines perform a wide variety of real-time analytics, transformations, and AI and machine learning on the data prior to storage:[77]



119. The diagram above confirms that Meta does not merely store incoming data for later review; rather, before the data is stored, Meta contemporaneously reads and processes it—including by reading the data, cleaning it, applying "real-time personalization" to associate it with a particular user, and analyzing its contents as necessary to generate real-time responses.

120. On information and belief, the other Third Parties also use ingest-phase processing platforms that perform real-time analytics and filtering on incoming data streams before storage. For example, Google developed MillWheel, an internal stream processing system, as well as Flume/FlumeJava, which evolved into Google Cloud Dataflow.[78] Google Cloud Dataflow enables Google to perform many functions on real-time data at the "Ingest" phase, before it is stored.[79] Google, which sells Dataflow to third-party developers for use with their own products, states that Dataflow is used "to create data pipelines that read from one or

---

[77] *Id.* at 2:05.
[78] *See, e.g.*, Google Cloud Blog, "How cloud batch and stream data processing works" (August 2020), https://cloud.google.com/blog/products/data-analytics/how-cloud-batch-and-stream-data-processing-works.
[79] Google Cloud Blog, "BigQuery explained: An overview of BigQuery's architecture" (September 2, 2020), https://cloud.google.com/blog/products/data-analytics/new-blog-series-bigquery-explained-overview.

more sources, ***transform the data***, and write the data to a destination."[80] One use for Dataflow is the "[r]eal-time machine learning (ML) analysis of streaming data."[81] Google confirms that Dataflow is "suitable for more advanced applications, such as real-time streaming analytics."[82]

121. Pinterest uses Apache Kafka, a third-party real-time stream processing platform.[83] The Kafka system streams events in real time to "many applications, such as native Kafka clients, Kafka Streams, Flink, and Spark streaming, which are consumers of a subset of Kafka topics that build several real-time pipelines."[84] These systems "include but are not limited to monetization, safety and spam detection, metrics processing, and experimentation use cases."[85]

122. Microsoft's Clarity also uses real-time stream processing software, which "processes millions of user sessions every day."[86] Although not as much is publicly disclosed about Microsoft's system, Microsoft confirms that the real-time data "is then sent to Clarity's backend, where it flows through a complex processing pipeline ***before*** ultimately being stored in ClickHouse—the powerful database that fuels Clarity's dashboards and visual reporting."[87]

123. Accordingly, the Third Parties' platforms do not operate as passive recipients that merely record user communications. Instead, they function as active interceptors that contemporaneously read and process the contents of user communications—including the Private Communications—by transforming, deduplicating, validating, filtering, and analyzing in real time while those communications are in transit between the user's browser and Defendant's Websites.

---

[80] Google Cloud Documentation, "Dataflow overview," https://docs.cloud.google.com/dataflow/docs/overview.
[81] *Id.*
[82] *Id.*
[83] Confluent, "Lessons Learned from Running Apache Kafka at Scale at Pinterest," https://www.confluent.io/blog/running-kafka-at-scale-at-pinterest/.
[84] *Id.*
[85] *Id.*
[86] Clarity Blog, "Building a Scalable Analytics Platform: Why Microsoft Clarity Chose ClickHouse," https://clarity.microsoft.com/blog/why-microsoft-clarity-chose-clickhouse/.
[87] *Id.*

E. The Private Communications Collected are Valuable.

124. As part of its regular course of business, Defendant targets California consumers by causing the Third Parties to extract, collect, maintain, distribute, and exploit, for Defendant's and the Third Parties' profit, all of the Private Communications transferred by the cookies which Defendant causes to be placed on Plaintiffs' and other California users' devices without their knowledge or consent. Defendant knew the location of consumers like Plaintiffs and the Class members either prior to or shortly after causing the Third Parties to use cookies on their devices.

125. The Private Communications tracked and collected through cookies on the Websites are valuable to Defendant and the Third Parties. Defendant uses this data to measure and optimize marketing campaigns, evaluate website design and product placement, and target specific users or groups of users with advertising. For example, Defendant can identify California users who visit webpages related to particular beverage products and then target those users with advertisements for similar products both on the Websites and across unrelated third-party websites.

126. Data reflecting users' browsing activity allows Defendant to identify behavioral patterns, preferences, and interests relating to Defendant's products. At scale, this data enables Defendant to assess trends across its brands and within the broader consumer beverage market. Defendant monetizes this data by leveraging it to increase user engagement, advertising effectiveness, and overall revenue.

127. The value of the Private Communications tracked and collected by the Third Parties using cookies on the Websites can be quantified. Legal scholars observe that "[p]ersonal information is an important currency in the new millennium."[88] Indeed, "[t]he monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend." *Id*. "Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information." *Id*.

128. Numerous empirical studies quantify the appropriate value measure for personal

[88] *See* Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004).

data. Generally, the value of personal data is measured as either the consumer's willingness to accept compensation to sell her data or the consumer's willingness to pay to protect her information.

129. By falsely representing consumers' ability to decline, reject, or opt out of unnecessary cookies, and by aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties to collect users' Private Communications, Defendant unjustly enriches itself at the expense of consumer privacy and autonomy. Defendant deprives consumers of the ability to decide whether, and on what terms, their data may be monetized.

PLAINTIFFS' EXPERIENCES

Plaintiff Miles

130. Plaintiff Miles visited Defendant's Websites, including the Coca-Cola, Sprite, and Vitaminwater Websites, on multiple occasions during the last four years, while located in California, to seek and obtain information about Defendant's products. Specifically, Plaintiff Miles visited the Websites to research various beverages, including their ingredients, nutritional information, flavors, and product varieties, and to look for coupons and promotions. Plaintiff Miles was particularly interested in Cherry Coke, tropical-flavored beverages and related coupons, Vitaminwater dragon fruit and energy varieties, and zero-sugar beverages.

131. Plaintiff Miles's visits to the Websites were consistent with an ordinary Website user's visits seeking information about Defendant's products. During her visits, Plaintiff Miles browsed beverage products and varieties, reviewed product and nutritional information, searched for coupons and promotions, and used the Websites' search features. Plaintiff Miles is not a consumer advocate, a "tester," or a compliance auditor who visited the Websites to test or evaluate Defendant's privacy practices.

132. When Plaintiff Miles visited the Websites, each Website immediately detected that she was a visitor in California and presented her with Defendant's popup cookie consent banner, which provided the option to adjust the toggle switches to decline, reject, or opt out of all unnecessary cookies, including the categories of Advertising, Analytics, and Personalization cookies. Plaintiff Miles viewed Defendant's representation on the popup cookie consent banner

that, "We use cookies to operate our website to show you personalized content and manage our objectives as a business. To change your preferences click manage settings below." Plaintiff Miles also viewed Defendant's additional representations, under the "Manage Settings" heading, that users could adjust the toggle switches to decline, reject, or opt out of all categories of cookies, including all Advertising, Analytics, and Personalization cookies, except "Necessary" cookies, which are "Always Active."

133. Plaintiff Miles adjusted the available toggle switches for each category of Advertising, Analytics, and Personalization cookies, except "Necessary" cookies, which she could not reject. Plaintiff Miles believed that adjusting the toggle switches on the popup cookie consent banner found on the Websites would allow her to decline, reject, or opt out of all unnecessary cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of tracking data to third-party advertising networks and/or analytics services for the purposes of providing personalized content, advertising, and analytics).

134. In adjusting the available toggle switches on the popup cookie consent banner, Plaintiff Miles gave Defendant notice that she did not consent to the use or placement of cookies and tracking technologies while browsing the Websites. Further, Plaintiff Miles specifically rejected, based on Defendant's representations, those cookies used to "show you personalized content and manage our objectives as a business" and share information with third parties for those and other purposes. Only after clicking or selecting the "Confirm my Choices" button did Plaintiff Miles, in reliance on these representations and promises, continue browsing the Websites.

135. Defendant caused cookies and tracking technologies, including those used for personalized content, advertising, and analytics, to be placed on Plaintiff Miles's device and/or intercepted by the Third Parties along with user data, without Plaintiff Miles's knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Miles that she could decline, reject, or opt out of the use and/or placement of all unnecessary cookies and tracking technologies while she browsed the Websites was false. Contrary to what Defendant made Plaintiff Miles believe, she did not have a choice about whether third-party cookies would be

placed on her device and/or intercepted by the Third Parties along with her user data; rather, Defendant had already caused that to happen.

136. Then, as Plaintiff Miles continued to browse the Websites in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff Miles's clear rejection of the use and/or placement of such cookies and tracking technologies, Defendant continued to cause the Third Parties' cookies, including those involved in providing personalized content, advertising, and analytics, to be placed on her device and/or transmitted along with user data. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Miles's Private Communications as Plaintiff Miles browsed the Websites.

137. Defendant's representations that, while browsing the Websites, consumers could decline, reject, or opt out of all categories of cookies other than "Necessary" cookies—or at least those involved in providing personalized content, advertising, and analytics—were untrue. Had Plaintiff Miles known this fact, she would not have interacted with the Websites. Moreover, Plaintiff Miles reviewed the popup cookie consent banner prior to using the Websites. Had Defendant disclosed that it would continue to cause cookies and tracking technologies to be stored on consumers' devices even after they choose to reject all unnecessary cookies, Plaintiff Miles would have noticed it and would not have used the Websites or, at a minimum, she would have interacted with the Websites differently.

138. Plaintiff Miles continues to desire to browse content featured on the Websites. Plaintiff Miles would like to browse websites that do not misrepresent that users can decline, reject, or opt out of all unnecessary cookies and tracking technologies. If the Websites were programmed to honor users' requests to reject all such cookies and tracking technologies, Plaintiff Miles would likely browse the Websites again in the future, but will not do so until then. Plaintiff Miles regularly visits websites that feature content similar to that of the Websites. Because Plaintiff Miles does not know how the Websites are programmed, which can change over time, and because she does not have the technical knowledge necessary to test whether the Websites honor users' requests to reject all unnecessary cookies and tracking technologies, Plaintiff Miles will be unable to rely on Defendant's representations when browsing the Websites

in the future absent an injunction that prohibits Defendant from making misrepresentations on the Websites. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Miles is not a software developer and has not received training with respect to HTTP network calls.

Plaintiff Mandler

139. Plaintiff Mandler visited Defendant's Websites, including the Coca-Cola, Diet Coke, Powerade, and Topo Chico Websites, on multiple occasions, while located in California, to seek and obtain information about Defendant's products. Specifically, Plaintiff Mandler visited the Websites to research various beverages, including their ingredients, nutritional information, and different varieties. Plaintiff Mandler was particularly interested in the types of sugars, sweeteners, and additives used in these beverages, including whether Coca-Cola products contained high-fructose corn syrup or cane sugar, whether Diet Coke contained aspartame, and the sugar content of Powerade and Topo Chico. Plaintiff Mandler also sought information about where to purchase Coca-Cola made with cane sugar and researched different manufacturing locations.

140. Plaintiff Mandler's visits to the Websites were consistent with an ordinary Website user's visits seeking information about Defendant's products. During his visits, Plaintiff Mandler browsed beverage categories, individual products, and flavors; reviewed product ingredients and nutritional information; searched for information about Coca-Cola products; and used Website features to locate nearby retailers carrying Coca-Cola made with cane sugar. Plaintiff Mandler also entered personal information into forms on the Websites, including, to the best of his recollection, his name, email address, telephone number, date of birth, and preferences; and responded to popup questions. Plaintiff Mandler is not a consumer advocate, a "tester," or a compliance auditor who visited the Coca-Cola Website to test or evaluate Defendant's privacy practices.

141. When Plaintiff Mandler visited the Websites, each Website immediately detected that he was a visitor in California and presented him with Defendant's popup cookie consent banner, which provided the option to adjust the toggle switches to decline, reject, or opt out of all unnecessary cookies, including the categories of Advertising, Analytics, and Personalization cookies. Plaintiff Mandler viewed Defendant's representation on the popup cookie consent banner that, "We use cookies to operate our website to show you personalized content and manage our objectives as a business. To change your preferences click manage settings below." Plaintiff Mandler also viewed Defendant's additional representations, under the "Manage Settings" heading, that users could adjust the toggle switches to decline, reject, or opt out of all categories of cookies, including all Advertising, Analytics, and Personalization cookies, except "Necessary" cookies, which are "Always Active."

142. Plaintiff Mandler adjusted the available toggle switches for each category of Advertising, Analytics, and Personalization cookies, except "Necessary" cookies, which he could not reject. Plaintiff Mandler believed that adjusting the toggle switches on the popup cookie consent banner found on the Websites would allow him to decline, reject, or opt out of all unnecessary cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of tracking data to third-party advertising networks and/or analytics services for the purposes of providing personalized content, advertising, and analytics).

143. In adjusting the available toggle switches on the popup cookie consent banner, Plaintiff Mandler gave Defendant notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Websites. Further, Plaintiff Mandler specifically rejected, based on Defendant's representations, those cookies used to "show you personalized content and manage our objectives as a business" and share information with third parties for those and other purposes. Only after clicking or selecting the "Confirm my Choices" button did Plaintiff Mandler, in reliance on these representations and promises, continue browsing the Websites.

144. Defendant caused cookies and tracking technologies, including those used for personalized content, advertising, and analytics, to be placed on Plaintiff Mandler's device

and/or intercepted by the Third Parties along with user data, without Plaintiff Mandler's knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Mandler that he could decline, reject, or opt out of the use and/or placement of all unnecessary cookies and tracking technologies while he browsed the Websites was false. Contrary to what Defendant made Plaintiff Mandler believe, he did not have a choice about whether third-party cookies would be placed on his device and/or intercepted by the Third Parties along with his user data; rather, Defendant had already caused that to happen.

145. Then, as Plaintiff Mandler continued to browse the Websites in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff Mandler's clear rejection of the use and/or placement of such cookies and tracking technologies, Defendant continued to cause the Third Parties' cookies, including those involved in providing personalized content, advertising, and analytics, to be placed on his device and/or transmitted along with user data. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Mandler's Private Communications as Plaintiff Mandler browsed the Websites.

146. Defendant's representations that, while browsing the Websites, consumers could decline, reject, or opt out of all categories of cookies other than "Necessary" cookies—or at least those involved in providing personalized content, advertising, and analytics—were untrue. Had Plaintiff Mandler known this fact, he would not have used the Websites. Moreover, Plaintiff Mandler reviewed the popup cookie consent banner prior to using the Websites. Had Defendant disclosed that it would continue to cause cookies and tracking technologies to be stored on consumers' devices even after they choose to reject all unnecessary cookies, Plaintiff Mandler would have noticed it and would not have used the Websites or, at a minimum, he would have interacted with the Websites differently.

147. Plaintiff Mandler continues to desire to browse content featured on the Websites. Plaintiff Mandler would like to browse websites that do not misrepresent that users can decline, reject, or opt out of all unnecessary cookies and tracking technologies. If the Websites were programmed to honor users' requests to reject all such cookies and tracking technologies, Plaintiff Mandler would likely browse the Websites again in the future, but will not do so until

then. Plaintiff Mandler regularly visits websites that feature content similar to that of the Websites. Because Plaintiff Mandler does not know how the Websites are programmed, which can change over time, and because he does not have the technical knowledge necessary to test whether the Websites honor users' requests to reject all unnecessary cookies and tracking technologies, Plaintiff Mandler will be unable to rely on Defendant's representations when browsing the Websites in the future absent an injunction that prohibits Defendant from making misrepresentations on the Websites. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Mandler is not a software developer and has not received training with respect to HTTP network calls.

CLASS ALLEGATIONS

148. Plaintiffs bring this Class Action Complaint on behalf of themselves and a proposed class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure. Plaintiffs seek to represent the following group of similarly situated persons, defined as follows:

> **Class**: All persons who browsed any of the Websites in the State of California after adjusting the toggle switches in the popup cookie consent banner to decline, reject, or opt out of Advertising, Analytics and, on the Websites where available, Personalization cookies.

149. This action has been brought and may properly be maintained as a class action against Defendant because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

150. **Numerosity:** Plaintiffs do not know the exact size of the Class, but they estimate that it is composed of more than 100 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action

rather than in individual actions will benefit the parties and the courts.

151. **Common Questions Predominate:** This action involves common questions of law and fact to the Class because each Class member's claim derives from the same unlawful conduct that led them to believe that Defendant would not cause third-party cookies to be placed on their browsers and devices and/or intercepted by third parties along with user data, after Class members chose to decline, reject, or opt out of all unnecessary cookies and tracking technologies on the Websites, and that Defendant would not permit third parties to track and collect Class members' Private Communications as Class members browsed the Websites.

152. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class are:

a. Whether Defendant's popup cookie consent banner represented to users that they could decline, reject, or opt out of all categories of cookies other than those "Necessary" for the Websites to function;

b. Whether that representation was false or misleading;

c. Whether, after users adjusted the toggle switches to reject all unnecessary cookies, Defendant caused the Third Parties' cookies to be placed on, retained on, or transmitted from users' browsers and devices;

d. Whether Defendant caused users' Private Communications to be transmitted to the Third Parties after users rejected all unnecessary cookies;

e. Whether the Third Parties read, attempted to read, or learned the contents or meaning of users' communications while those communications were in transit;

f. Whether Defendant aided, agreed with, employed, permitted, or caused the Third Parties' conduct within the meaning of California Penal Code § 631(a);

g. Whether Class members had a reasonable expectation of privacy in their Private Communications on the Websites after rejecting unnecessary cookies;

h. Whether Defendant's conduct was highly offensive to a reasonable person

and constituted a serious invasion of privacy;

i. Whether Defendant knew, or was reckless in not knowing, that its representations were false;

j. Whether Defendant was unjustly enriched by the collection and use of Class members' Private Communications;

k. Whether Plaintiffs and Class members are entitled to statutory damages under California Penal Code § 637.2; and

l. Whether Plaintiffs and Class members are entitled to damages, restitution, injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest, and costs of suit.

153. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, Plaintiffs, like the other Class members, visited at least one of the Websites, adjusted the toggle switches to decline, reject, or opt out of all categories of unnecessary cookies, including all Advertising, Analytics, and Personalization cookies, and had their confidential Private Communications intercepted by the Third Parties.

154. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the interests of all Class members because it is in their best interests to prosecute the claims alleged herein to obtain full compensation due to them for the unfair and illegal conduct of which they complain. Plaintiffs also have no interests in conflict with, or antagonistic to, the interests of Class members. Plaintiffs have retained highly competent and experienced class action attorneys to represent their interests and those of the Class. By prevailing on their claims, Plaintiffs will establish Defendant's liability to all Class members. Plaintiffs and their counsel have the necessary financial resources to adequately and vigorously litigate this class action, and Plaintiffs and counsel are aware of their fiduciary responsibilities to the Class members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for Class members.

155. **Superiority:** There is no plain, speedy, or adequate remedy other than by maintenance of this class action. The prosecution of individual remedies by members of the Class

will tend to establish inconsistent standards of conduct for Defendant and result in the impairment of Class members' rights and the disposition of their interests through actions to which they were not parties. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. Furthermore, as the damages suffered by each individual member of the Class may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the Class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

First Cause of Action: Invasion of Privacy

156. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

157. To plead an invasion of privacy claim, Plaintiffs must show an invasion of (i) a legally protected privacy interest; (ii) a reasonable expectation of privacy in the circumstances; and (iii) conduct by Defendant constituting a serious invasion of privacy.

158. Defendant has intruded upon the following legally protected privacy interests of Plaintiffs and Class members: (i) the California Invasion of Privacy Act ("CIPA"), as alleged herein; (ii) the California Constitution, which guarantees Californians the right to privacy; and (iii) Cal. Penal Code § 484(a), which prohibits the knowing theft or defrauding of property "by any false or fraudulent representation or pretense."

159. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as Defendant affirmatively promised users they could decline, reject, or opt out of all categories of Advertising, Analytics, and Personalization cookies, except "Necessary" cookies, and similar tracking technologies before proceeding to browse the Websites. Plaintiffs and other Class members directed their electronic devices to access the Websites and, when presented with the popup cookie consent banner on the Websites, Plaintiffs and Class members

rejected all unnecessary cookies and reasonably expected that their rejection of such cookies and tracking technologies would be honored. That is, they reasonably believed that Defendant would not permit the Third Parties to store and send cookies and/or use other such tracking technologies on their devices while they browsed the Websites. Plaintiffs and Class members also reasonably expected that, if they declined, rejected, or opted out of such cookies and/or tracking technologies, Defendant would not permit the Third Parties to track and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, on the Websites.

160. Such information is "personal information" under California law, which defines personal information as including "[i]nternet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Penal Code § 1798.140.

161. Defendant, in violation of Plaintiffs' and other Class members' reasonable expectation of privacy and without their consent, permits the Third Parties to use cookies and other tracking technologies to collect, track, and compile users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is located in California. The data that Defendant allowed the Third Parties to collect enables the Third Parties to (and they in fact do), *inter alia*, create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; create audience segments based on shared traits (such as Millennials, Californians, tech enthusiasts, etc.); and perform targeted advertising and marketing analytics. Further, the Third Parties share user data and/or the user profiles with unknown parties to further their financial gain. The consumer profiles are, and can be, used to further invade Plaintiffs' and users' privacy, by allowing third parties to learn intimate details of their lives, and target them for advertising and other purposes,

as described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them.

162. Defendant's actions constituted a serious invasion of privacy in that they invaded a zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and violated criminal laws on wiretapping and invasion of privacy. These acts constitute an egregious breach of social norms that is highly offensive to a reasonable person.

163. Defendant lacked a legitimate business interest in causing the placement and/or transmission of third-party cookies along with user data that allowed the Third Parties to track, intercept, receive, and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, without their consent.

164. Plaintiffs and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

165. Plaintiffs and Class members seek appropriate relief for that injury, including, but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs' and Class members' privacy.

166. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' rejection of the Websites' use of all categories of cookies, including all Advertising, Analytics, and Personalization cookies (except "Necessary" cookies). Punitive damages are warranted to deter Defendant from engaging in future misconduct.

<u>Second Cause of Action</u>: Intrusion Upon Seclusion

167. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

168. To assert a claim for intrusion upon seclusion, Plaintiffs must plead (i) that Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs had

a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable person.

169. By permitting third-party cookies to be stored on consumers' devices without consent, which caused the Third Parties to track and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, contrary to Defendant's representations in the popup cookie consent banner, Defendant intentionally intruded upon the solitude or seclusion of the Websites' users. Defendant effectively placed the Third Parties in the middle of communications to which they were not invited, welcomed, or authorized.

170. The Third Parties' tracking and collecting of Plaintiffs' and Class members' Private Communications on the Websites using third-party cookies that Defendant causes to be stored on users' devices—and to be intercepted by Third Parties—was not authorized by Plaintiffs and Class members, and, in fact, those users specifically chose to decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies, except the "Necessary" cookies users could not reject.

171. Plaintiffs and the Class members had an objectively reasonable expectation of privacy surrounding their Private Communications on the Websites based on Defendant's promise that users could decline, reject, or opt out of all unnecessary cookies, as well as state criminal and civil laws designed to protect individual privacy.

172. Defendant's intentional intrusion into Plaintiffs' and other users' Private Communications would be highly offensive to a reasonable person given that Defendant represented that the Websites' users could decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies, except the "Necessary" cookies users could not reject, when, in fact, Defendant causes such third-party cookies to be stored on consumers' devices and browsers, and to be intercepted by third parties, even when consumers declined, rejected, or opted out of all such cookies. Indeed, Plaintiffs and

Class members reasonably expected, based on Defendant's false representations, that when they rejected all such cookies and tracking technologies, Defendant would not cause such third-party cookies to be stored on their devices or permit the Third Parties to obtain their Private Communications on the Websites, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is located in California.

173. Defendant's conduct was intentional and intruded on Plaintiffs' and users' Private Communications on the Websites.

174. Plaintiffs and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

175. Plaintiffs and Class members seek appropriate relief for that injury, including, but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs' and Class members' privacy.

176. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' rejection of the Websites' use of all unnecessary cookies, including Advertising, Analytics, and Personalization cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631)

177. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

178. California Penal Code § 631(a) provides, in pertinent part:

> "Any person [i] who, by means of any machine, instrument, or contrivance, or in any other manner intentionally taps, or makes any unauthorized connection … or [ii] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any

> place within this state; or [iii] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [iv] who aids, 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, is punishable by a fine not exceeding two thousand five hundred dollars . . . ."

179. Defendant is a "person" within the meaning of Cal. Penal Code § 631.

180. The Third Parties' cookies—as well as the software code of the Third Parties responsible for placing the cookies and transmitting data from user devices to the Third Parties—constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA (and, even if they do not, Defendant's deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of "any other manner").

181. Each of the Third Parties is a separate legal entity that provides software-as-a-service functionality and not merely a passive device. Further, the Third Parties had the capability to use the wiretapped information for their own purposes and, as alleged above, they did in fact use the wiretapped information for their own business purposes. Accordingly, the Third Parties were third parties to any communication between Plaintiffs and Class members, on the one hand, and Defendant, on the other.

182. Under § 631(a), Defendant must show it had the consent of all parties to a communication.

183. At all relevant times, the Websites caused Plaintiffs' and Class members' browsers to store the Third Parties' cookies and to transmit those cookies alongside Private Communications—including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—to the Third Parties without Plaintiffs' and Class members' consent. By configuring the Websites in this manner, Defendant willfully aided, agreed with, employed, permitted, or otherwise caused the Third Parties to wiretap Plaintiffs and Class members using the Third Parties' cookies and to accomplish the wrongful conduct alleged herein.

184. At all relevant times, by their cookies and corresponding software code, the Third Parties willfully and without the consent of all parties to the communication, or in any

unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiffs and Class members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

185. The Private Communications of Plaintiffs and Class members, on the one hand, and Defendant, on the other, that the Third Parties automatically intercepted directly communicate the Websites' users' affirmative decisions, actions, choices, preferences, and activities, which constitute the "contents" of electronic communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is located in California.

186. At all relevant times, the Third Parties used or attempted to use the Private Communications automatically intercepted by their cookie tracking technologies for their own purposes.

187. Plaintiffs and Class members did not provide their prior consent to the Third Parties' intentional access, interception, reading, learning, recording, collection, and usage of Plaintiffs' and Class members' electronic communications. Nor did Plaintiffs and Class members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties' conduct. On the contrary, Plaintiffs and Class members expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic communications by choosing to decline, reject, or opt out of all categories of Advertising, Analytics, and Personalization cookies, except those "Necessary" for the Websites to function, by adjusting the toggle switches in the consent banner.

188. The wiretapping of Plaintiffs and Class members occurred in California, where Plaintiffs and Class members accessed the Websites and where Defendant caused Plaintiffs' and Class members' electronic communications to be routed to the Third Parties' servers. Among

other things, the cookies, as well as the software code responsible for placing the cookies and transmitting them and other Private Communications to the Third Parties, resided on Plaintiffs' California-located devices. In particular, the user's California-based device, after downloading the software code from the Third Parties' servers, (i) stored the code onto the user's disk; (ii) converted the code into machine-executable format; and (iii) executed the code, causing the transmission of data (including cookie data) to and from the Third Parties.

189. Plaintiffs and Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of their right to privacy, (ii) loss of value in their Private Communications, (iii) damage to and loss of Plaintiffs' and Class members' property right to control the dissemination and use of their Private Communications, and (iv) loss of their Private Communications to the Third Parties with no consent.

190. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and Class members have been injured by the violations of Cal. Penal Code § 631, and each seeks statutory damages of the greater of $5,000, or three times the amount of actual damages, for each of Defendant's violations of CIPA § 631(a), as well as injunctive relief.

191. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein including, but not limited to, permitting third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Plaintiffs, Class members, and the general public continue to be at risk because Plaintiffs, Class members, and the general public frequently use the internet to search for information and content related to beverage products. Plaintiffs, Class members, and the general public continue to desire to use the internet for that purpose. Plaintiffs, Class members, and the general public have no practical way to know whether their request to decline, reject, or opt out of all categories of Advertising, Analytics, and Personalization cookies and tracking technologies will be honored and/or whether Defendant will permit third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic

Private Communications with Defendant and will continue to do so unless and until enjoined.

Fourth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation

192. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

193. Defendant fraudulently and deceptively informed Plaintiffs and Class members that they could decline, reject, or opt out of all categories of Advertising, Analytics, and Personalization cookies in use on the Websites, except those cookies "Necessary" for the Websites to function.

194. However, despite Defendant's representations otherwise, Defendant causes third-party cookies and software code to be stored on consumers' devices, and to be intercepted by the Third Parties alongside Private Communications, even after users adjust the available toggle switches in the popup cookie consent banner to decline, reject, or opt out of all such cookies. These cookies and corresponding software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' Private Communications, even when consumers had previously chosen to reject all unnecessary cookies.

195. Defendant affirmatively chose to deploy a cookie consent banner governing the collection, sharing, and use of users' Private Communications on the Websites.

196. By implementing the cookie banner, Defendant undertook responsibility for ensuring that the banner accurately communicated users' privacy choices and properly effectuated those choices.

197. Defendant and/or its agents configured and managed which technologies loaded and transmitted data before and after a user adjusted the toggle switches to reject all unnecessary cookies, including through consent management settings and/or platforms, tag-management rules, and related implementation choices under Defendant's control. On information and belief, Defendant operated, controlled, configured, approved, or maintained settings that permitted the Third Parties' tracking technologies to continue collecting users' Private Communications even after users adjust the available toggle switches to indicate their choice to decline, reject, or opt out of all categories of cookies in use on the Websites, including all Advertising, Analytics, and Personalization cookies (except those "Necessary Cookies" needed for the Websites to function).

198. Industry documentation for the consent management platforms and Third Parties' technologies used on the Websites explains that website operators, i.e., Defendant, must affirmatively configure consent settings and tag behavior to prevent tracking technologies from firing after users reject cookies. On information and belief, Defendant received, reviewed, or had access to such implementation guidance in deploying the challenged technologies on the Websites. On information and belief, Defendant had the ability during the relevant time period to audit, test, configure, disable, or modify the cookie consent banner, consent-management functionality, and third-party tracking technologies operating on the Websites. Defendant had information available to it demonstrating that users' purported opt-out selections were not being honored and that users' Private Communications continued to be collected and intercepted by the Third Parties notwithstanding Defendant's contrary representations.

199. Defendant also used the Third Parties' analytics, advertising, and reporting dashboards to monitor the Websites' traffic, user behavior, advertising performance, and related engagement metrics generated through the challenged cookie and tracking technologies. Through these dashboards and related reporting tools, Defendant had access to information reflecting that user data continued to be intercepted by and processed by the Third Parties notwithstanding users' purported opt-out selections. Defendant routinely reviewed, monitored, and relied upon data generated through the Third Parties' resources for advertising, analytics, personalization, attribution, and/or website performance purposes.

200. Industry standards, privacy frameworks, and applicable statutes and regulations, including the California Consumer Privacy Act and related regulations, require website operators deploying cookie consent banners to ensure that consent mechanisms function properly and accurately record and enforce user choices. *See*, *e.g.*, Cal. Code Regs. tit. 11, § 7025(c) (enumerating requirements for businesses that receive an "opt out preference signal."); *id*. § 7101 (business record keeping requirements regarding opt out requests).

201. On information and belief, Defendant either knew its representations regarding users' ability to decline, reject, or opt out of all categories of cookies in use on the Websites (other than those "Necessary" for the Websites to function) were false, lacked any reasonable

basis for believing those representations were true, or made those representations carelessly and recklessly despite information available to Defendant demonstrating that users' data continued to be collected and intercepted by the Third Parties after users attempted to opt out.

202. These misrepresentations and omissions were known exclusively to, and actively concealed by, Defendant, not reasonably known to Plaintiffs and Class members, and material at the time they were made. Defendant's misrepresentations and omissions concerned material facts that were essential to the analysis undertaken by Plaintiffs and Class members as to whether to use the Websites. In misleading Plaintiffs and Class members and not so informing them, Defendant breached its duty to Plaintiffs and Class members. Defendant also gained financially from, and as a result of, its breach.

203. Plaintiffs and Class members have suffered an injury as a result of the Third Parties' unauthorized interception of their Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, which have value as demonstrated by the use and sale of consumers' browsing activity, as alleged above. Plaintiffs and Class members have also suffered harm in the form of diminution of the value of their private and personally identifiable information and communications.

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

205. Defendant's representation that consumers could decline, reject, or opt out of all categories of Advertising, Analytics, and Personalization cookies (including "cookies [used] to operate our website to show you personalized content and manage our objectives as a business"), except "Necessary" cookies, if they adjusted the toggle switches to do so was untrue. Again, had Plaintiffs and Class members known these facts, they would not have used the Websites. Moreover, Plaintiffs and Class members reviewed the popup cookie consent banner prior to their interactions with the Websites. Had Defendant disclosed that it caused unnecessary third-party

cookies to be stored on the Websites' visitors' devices relating to advertising, analytics, and personalization and/or that it shared information with third parties even after they choose to decline, reject, or opt out of all such cookies, Plaintiffs and Class members would have noticed it and would not have interacted with the Websites.

206. By and through such fraud, deceit, misrepresentations and/or omissions, Defendant intended to induce Plaintiffs and Class members to alter their positions to their detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiffs and Class members to, without limitation, use the Websites under the mistaken belief that Defendant would not permit third parties to obtain users' Private Communications when consumers chose to decline, reject, or opt out of all unnecessary cookies. As a result, Plaintiffs and the Class provided more personal data than they would have otherwise.

207. Plaintiffs and Class members justifiably and reasonably relied on Defendant's misrepresentations and fraudulent omissions, and, accordingly, were damaged by Defendant's conduct.

208. As a direct and proximate result of Defendant's misrepresentations and/or omissions, Plaintiffs and Class members have suffered damages, as alleged above, and are entitled to just compensation, including monetary damages.

209. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' rejection of the Websites' use of all categories of Advertising, Analytics, and Personalization cookies, except those cookies "Necessary" for the Websites to function. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Fifth Cause of Action: Unjust Enrichment

210. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

211. Defendant created and implemented a scheme to increase its own profits through a pervasive pattern of false statements and fraudulent omissions.

212. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could decline, reject, or opt out of all categories of Advertising, Analytics, and Personalization cookies, except those cookies "Necessary" for the Websites to function, and by permitting the Third Parties to store and transmit cookies on Plaintiffs' and Class members' devices and browsers, which permitted the Third Parties to track and collect users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even after Class members rejected all unnecessary cookies.

213. Plaintiffs' and Class members' Private Communications have conferred an economic benefit on Defendant.

214. Defendant has been unjustly enriched at the expense of Plaintiffs and Class members, and Defendant has unjustly retained the benefits of its unlawful and wrongful conduct.

215. Defendant appreciated, recognized, and chose to accept the monetary benefits that Plaintiffs and Class members conferred upon Defendant to their detriment. These benefits were the expected result of Defendant acting in its pecuniary interest at the expense of Plaintiffs and Class members.

216. It would be unjust for Defendant to retain the value of Plaintiffs' and Class members' property and any profits earned thereon.

217. There is no justification for Defendant's enrichment. It would be inequitable, unconscionable, and unjust for Defendant to be permitted to retain these benefits because the benefits were procured as a result of its wrongful conduct.

218. Plaintiffs and Class members are entitled to restitution of the benefits Defendant unjustly retained and/or any amounts necessary to return Plaintiffs and Class members to the position they occupied prior to having their Private Communications tracked and collected by the Third Parties.

219. Plaintiffs plead this claim separately, and in the alternative to their other claims, to the extent those claims do not provide an adequate legal remedy.

PRAYER FOR RELIEF

WHEREFORE, reserving all rights, Plaintiffs, on behalf of themselves and the Class members, respectfully request judgment against Defendant as follows:

A. Certification of the proposed Class, Plaintiffs as class representatives, and appointment of Plaintiffs' counsel as class counsel;

B. An award of compensatory damages, including statutory damages where available, to Plaintiffs and Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, including both pre- and post-judgment interest thereon;

C. An award of punitive damages;

D. An award of nominal damages;

E. An order for full restitution;

F. An order requiring Defendant to disgorge revenues and profits wrongfully obtained;

G. An order temporarily and permanently enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

H. An award of reasonable attorneys' fees and the costs of suit incurred; and

I. For such further relief as may be just and proper.

Dated: November 6, 2026

GUTRIDE SAFIER LLP

/s/ Seth A. Safier

Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie A. McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiffs

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Coca-Cola Disregards Website Visitors' Cookie Preferences, Class Action Lawsuit Alleges