UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

LAURA GILBERT, individually and on behalf of all others similarly situated, Plaintiff, v. BROOKLINEN, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Laura Gilbert ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her undersigned counsel, bring this Class Action Complaint against Defendant Brooklinen, Inc. ("Defendant" or "Brooklinen"). Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. In recent years, federal courts across the country have warned that opaque digital-tracking practices pose a profound threat to Americans' privacy. The unauthorized collection of a person's browsing activity, website interactions, and device identifiers constitutes an invasion of the most basic expectation of privacy in one's online life. When a company affirmatively represents that users may control whether their data is sold, shared, or tracked, but then secretly sells, shares, and tracks that data anyway, the misconduct is especially egregious.

2. Brooklinen owns, operates, and controls the website located at https://www.brooklinen.com (the "Website"), through which it operates an online retail platform offering bedding, bath, loungewear, home décor, and related household products, processes

consumer purchases, manages customer accounts and promotional programs, and provides product, pricing, and related content to consumers nationwide.

3. Like many modern websites, the Website displays a Cookie banner (the "Cookie Banner") and a "cookie preferences" interface (the "Cookie Settings") purporting to give users meaningful control over what data the Website shares with third parties. The Cookie Banner as shown to users in California, and the Cookie Settings are shown below:

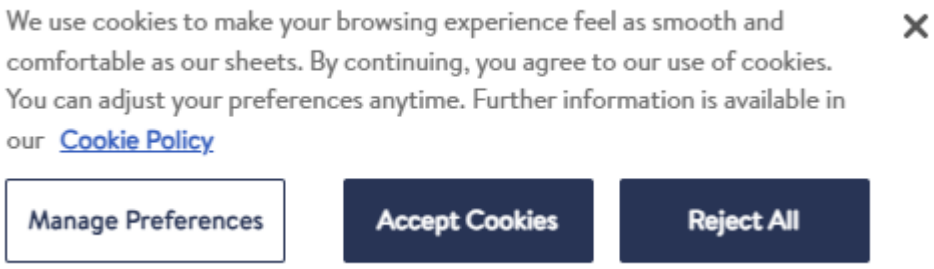


Figure 1 – Brooklinen's Cookie Banner, representing that users may opt out of the sale or sharing of their personal information by selecting "Manage Preferences"

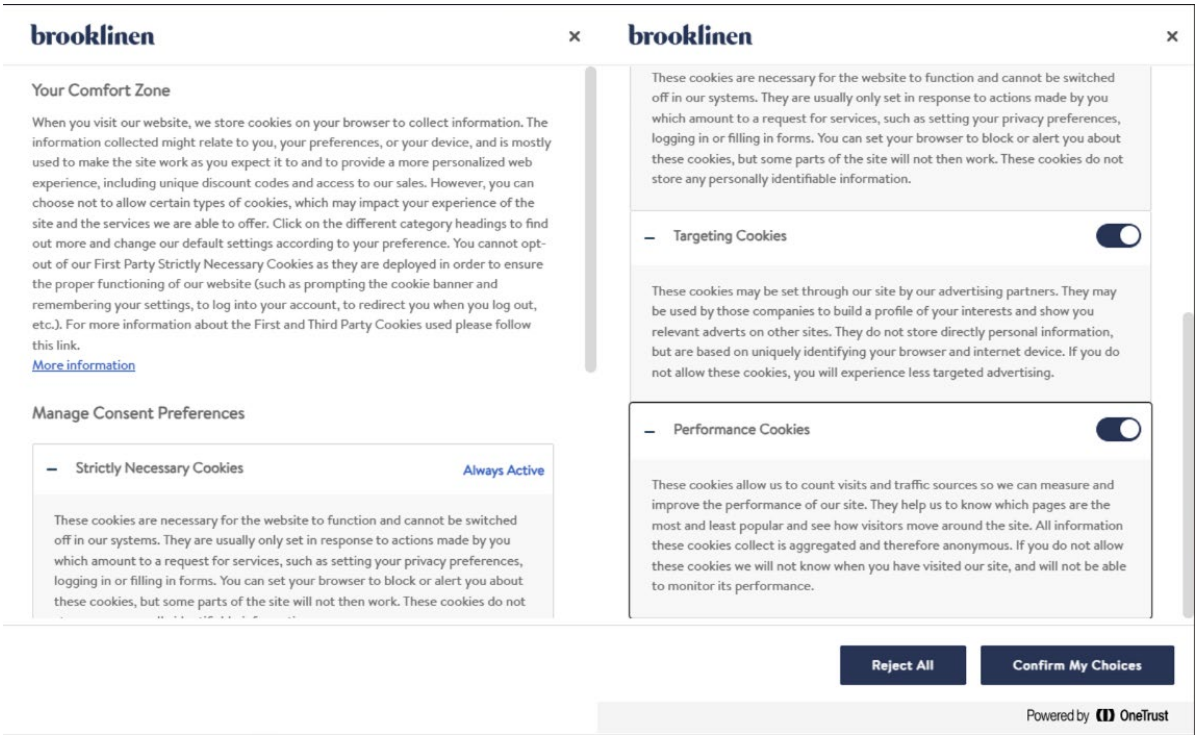


Figure 2 – Cookie Settings of Website

4. Defendant's assurances are false. The Website begins placing and transmitting cookies and other third-party tracking technologies (the "Tracking Tools") capable of transmitting users' data the moment users visit the Website, before they can interact with the Cookie Banner or select their preferences in the Cookie Settings.

5. Worse still, even after users affirmatively reject all non-necessary cookies, the Website continues to utilize and deploy Tracking Tools which transmit users' data to the advertising, social media, and analytics companies that designed and operate the Tracking Tools, including Facebook, TikTok, Google, Microsoft, Pinterest, Snapchat, and Reddit (the "Tracking Entities").

6. Brooklinen's Cookie Banner and Cookie Settings deceive users by (1) placing Tracking Tools on users' browsers, which allow Tracking Entities to intercept users' communications with the Website before users have the ability to interact with the Cookie Banner, and by (2) continuing to use Tracking Tools that intercept and transmit user data to Tracking Entities after users reject all non-necessary cookies.

7. Misrepresenting the effectiveness of a cookie opt-out mechanism effectively deprives users of control over their personal information.

8. The Tracking Tools intercept, copy, and transmit detailed interaction and behavioral data, including users' selections of links, buttons, forms, and other on-page elements, as well as information entered into search fields. This data may include webpages and products viewed or purchased; inferred interests, preferences, age, location, or other characteristics based on user behavior and content engagement; and personal, device, and technical identifiers such as device type, operating system, and browser type. The data also includes persistent identifiers that enable recognition of users across sessions and websites, users' email addresses, and approximate

geolocation information derived from IP addresses or similar signals. Collectively, this information is referred to as "Sensitive Information." This Sensitive Information is collected regardless of whether users reject non-essential cookies.

9. In short, the Website's Cookie Banner and Cookie Settings materially mislead users about the use and sale of their data. Defendant lulls users into a false sense of security, privacy, and control while simultaneously enabling third parties to monitor, intercept, and transmit users' online behavior in real time. Such conduct deprives users of control over their personal information and violates fundamental privacy protections.

10. Plaintiff's experiences reflect the conduct described above. Plaintiff, a resident of California, visited Defendant's Website in May 2026, respectively, for ordinary consumer purposes, including browsing content and products such as covers and robes, and otherwise navigating the Website's content.

11. While accessing the Website from her state of residence, Plaintiff encountered the Website's Cookie Banner and Cookie Settings. Plaintiff affirmatively rejected non-essential cookies, relying on Defendant's representations that Tracking Tools would not be deployed by the Website without her consent. Despite these actions and expectations, the Website deployed Tracking Tools that automatically intercepted Plaintiff's Sensitive Information and transmitted Plaintiff's Sensitive Information to the Tracking Entities.

12. In each instance, Plaintiff reasonably relied on Defendant's representations regarding data privacy controls and privacy protections, yet her Sensitive Information was nonetheless collected and shared against her express rejections. Plaintiff was thereby subjected to unauthorized disclosure of her communications and deprived of the privacy benefits that Defendant represented users could obtain by rejecting the use of Tracking Tools.

13. Defendant invaded Plaintiff's fundamental rights to privacy and fraudulently misrepresented the Website's data-collection practices by facilitating the Tracking Entities' unlawful interception of and intrusion into Plaintiff's Sensitive Information. In doing so, Defendant violated the federal Wiretap Act, 18 U.S.C. § 2510, et seq.; California's Invasion of Privacy Act ("CIPA"), including Cal. Penal Codes §§ 631 (illegal wiretapping) and 638.51 (unlawful use of a pen register or trap and trace device); California's Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750, et seq.; California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq.; and common law, including fraud and deceit, negligent misrepresentation, and unjust enrichment. Plaintiff brings this action on behalf of herself and a putative class of similarly situated persons who were harmed by Defendant's deceptive and unlawful surveillance practices.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under the federal Wiretap Act, 18 U.S.C. § 2510, et seq. This Court has supplemental jurisdiction over the non-federal claims in this action. This Court also has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is more than 100, and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

15. This Court has personal jurisdiction over Defendant because Defendant is registered to do business in this District and maintains its principal place of business in this District.

16. Venue is proper in this Court because Defendant's principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

17. Plaintiff Laura Gilbert is, and at all relevant times has been, a citizen and resident of the State of California. Plaintiff Gilbert accessed and used Defendant's Website while physically located in California. Most recently, Plaintiff Gilbert visited Defendant's Website in or about May 2026 for consumer purposes, including browsing merchandise, specifically robes and sheets offered on Defendant's Website. During her visit, Plaintiff Gilbert reviewed product pages "Bed" and "Bath." Plaintiff consistently rejects the use of Tracking Tools on all websites she visits as a matter of personal privacy practice. In connection with her visit to Defendant's Website, Plaintiff Gilbert was presented with the Website's Cookie Banner offering the options "Manage Preferences," "Reject All," and "Accept Cookies." Plaintiff Gilbert engaged with the Cookie Banner and affirmatively rejected all non-essential cookies in reliance on Defendant's representations that doing so would disable technologies such as cookies. Plaintiff Gilbert reasonably believed that by rejecting, her browsing activity would not be tracked beyond what was strictly necessary for the Website's basic functionality. Despite Plaintiff Gilbert's affirmative rejection of non-essential tracking technologies, Defendant deployed Tracking Tools that intercepted and recorded Plaintiff Gilbert's browsing activity, device identifiers, and related metadata, simultaneously transmitting the intercepted data to Tracking Entities. The intercepted communications disclosed the substance of Plaintiff Gilbert's communications with the Website, including her Sensitive Information. Had Plaintiff Gilbert known that she could not rely on

Defendant's representations regarding Tracking Tools, she would not have navigated to, browsed, or used the Defendant's Website.

18. Defendant Brooklinen, Inc. is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business located at 225 Varick Street, Suite 800, New York, New York 10014. Brooklinen conducts business throughout New York and the United States, including through its ownership, operation, and control of the Website, an online retail platform through which consumers may browse and purchase bedding, bath products, home furnishings, loungewear, and related merchandise, create and maintain user accounts, and access prerecorded audiovisual content.

FACTUAL ALLEGATIONS

I. How Websites Function

19. Websites are hosted on servers, in the sense that their files are stored on and accessed from servers. Websites are, in part, "run" on a user's internet browser, as the browser loads and processes the website's code to display the webpage.

20. Websites are a collection of webpages. A webpage is essentially a document containing text written in HyperText Markup Language (HTML) code.[1]

21. Each webpage has a unique address, and two webpages cannot be stored at the same address.[2]

22. When a user navigates to a webpage (by entering a URL address directly or clicking a hyperlink containing the address[3]), that user's browser contacts a DNS (Domain Name

[1] *Browsing the web: What is the difference between webpage, website, web server, and search engine?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/Pages_sites_servers_and_search_engines (last visited May 7, 2026).
[2] *Id.*
[3] A URL address is created and named by a website developer.

System) server, which translates the website's web address into a unique IP (Internet Protocol) address.[4]

23. An IP address is "a unique address that identifies a device on the Internet or a local network."[5] In essence, an IP address is defined as follows:

> The identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.[6]

24. When a user's browser navigates to a webpage, it sends an HTTP request to the server identified by the webpage's IP address (the "Request URL"). This request is for the specific resource located at the URL. If the server fulfills this request, it issues an HTTP response that includes the request status and, typically, the requested content. This content is then transmitted in small chunks, known as data packets, and reassembled into the complete webpage by the user's browser upon arrival.[7]

25. This Request URL includes a domain name and path, which identify the specific content being accessed on a website and its location within the website's structure.

26. The Request URL typically contains parameters. Parameters are values added to a URL to transmit data to the recipient, prefaced by a question mark to signal the use of parameters. Parameters direct a web server to provide additional context-sensitive services,[8] as depicted below:

---

[4] *How the web works*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited May 7, 2026).
[5] *What is an IP Address – Definition and Explanation*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/what-is-an-ip-address (last visited May 7, 2026).
[6] *Id.*
[7] *Id.*
[8] To see examples of how Defendant used parameters to provide additional information here, *see, infra,* Section C(2).

Figure 3 – Mozilla's diagram of a URL, including parameters[9]

27. Website owners or web developers write and manage the URLs for their websites.

28. URL encoding is an essential process to ensure that data is safely transmitted via URLs. URL encoding converts characters into a format that can be transmitted over the Internet.[10] For example, URLs cannot contain spaces; URL encoding normally replaces a space with a plus (+) sign or with %20.

29. The American Standard Code for Information Interchange (ASCII) was designed in the early 1960s as a standard character set for computers and electronic devices.[11] Today, UTF-8 is the Internet's most common character encoding.[12]

30. URL decoding is the process of URL encoding in reverse so that the URL is in a more readable format.[13] To demonstrate:

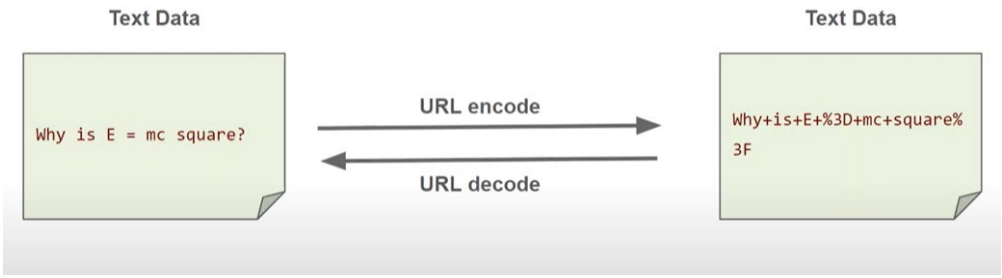


Figure 4 – Demonstrating URL encoding and decoding.[14]

---

[9] *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited May 7, 2026).
[10] *Id.*
[11] *HTML ASCII Reference*, W3 SCHOOLS, https://www.w3schools.com/charsets/ref_html_ascii.asp (last visited May 7, 2026).
[12] *UTF-8*, MOZILLA, https://developer.mozilla.org/en-US/docs/Glossary/UTF-8 (last visited May 7, 2026).
[13] *What Is URL Decoding and URL Encoding?*, GOCHYU (last modified Oct. 18, 2020) https://gochyu.com/blog/url-encode-decode (last visited May 7, 2026).
[14] Viraj Shetty, *URL Encoding in a few minutes*, YOUTUBE (Sept. 5, 2023) https://www.youtube.com/watch?v=ru0iCHsmsLc (last visited May 7, 2026).

31. Similarly, parameters and metadata can be parsed and separated into easily reviewed, searchable formats.

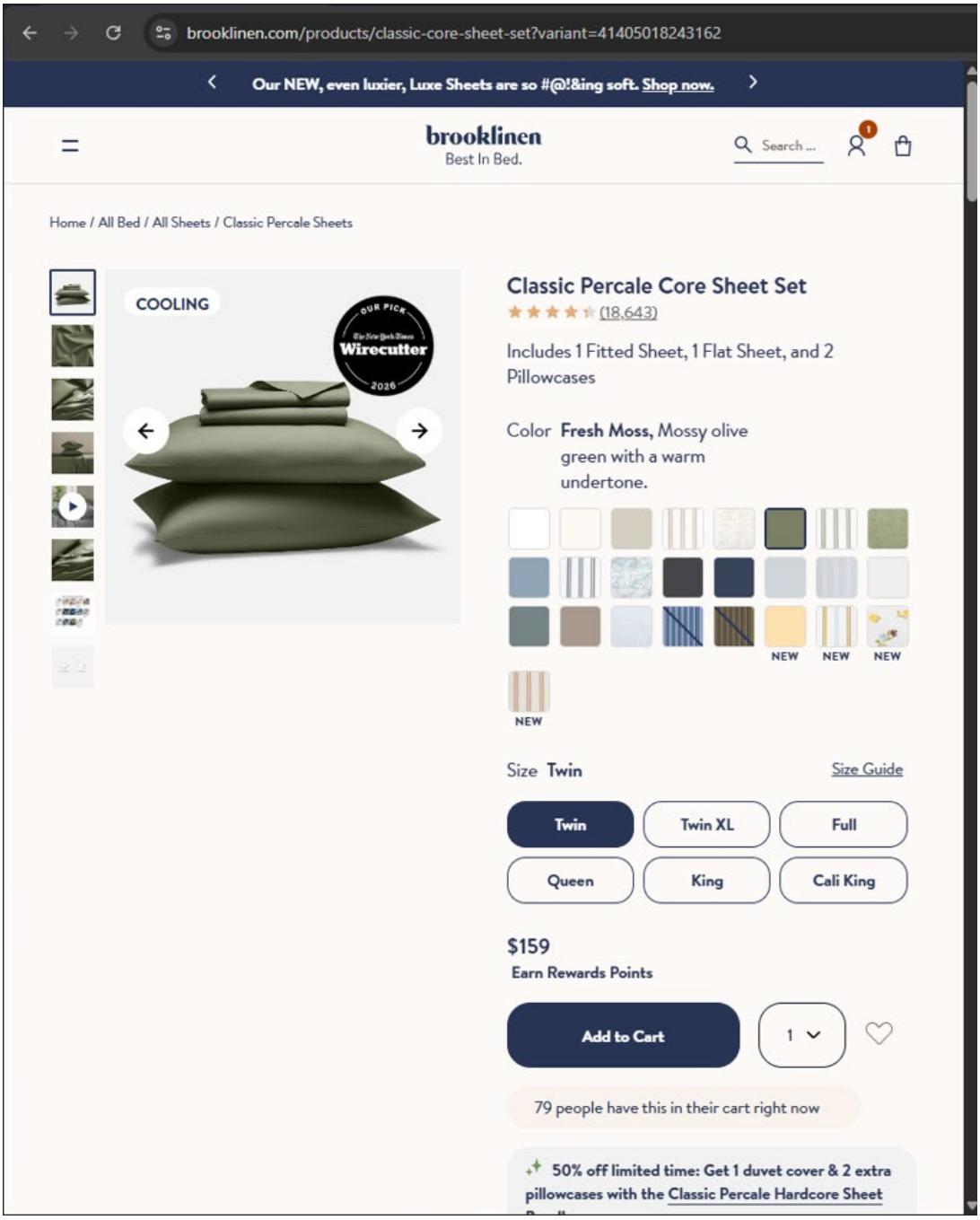


Figure 5 – Sample webpage used to demonstrate a webpage URL

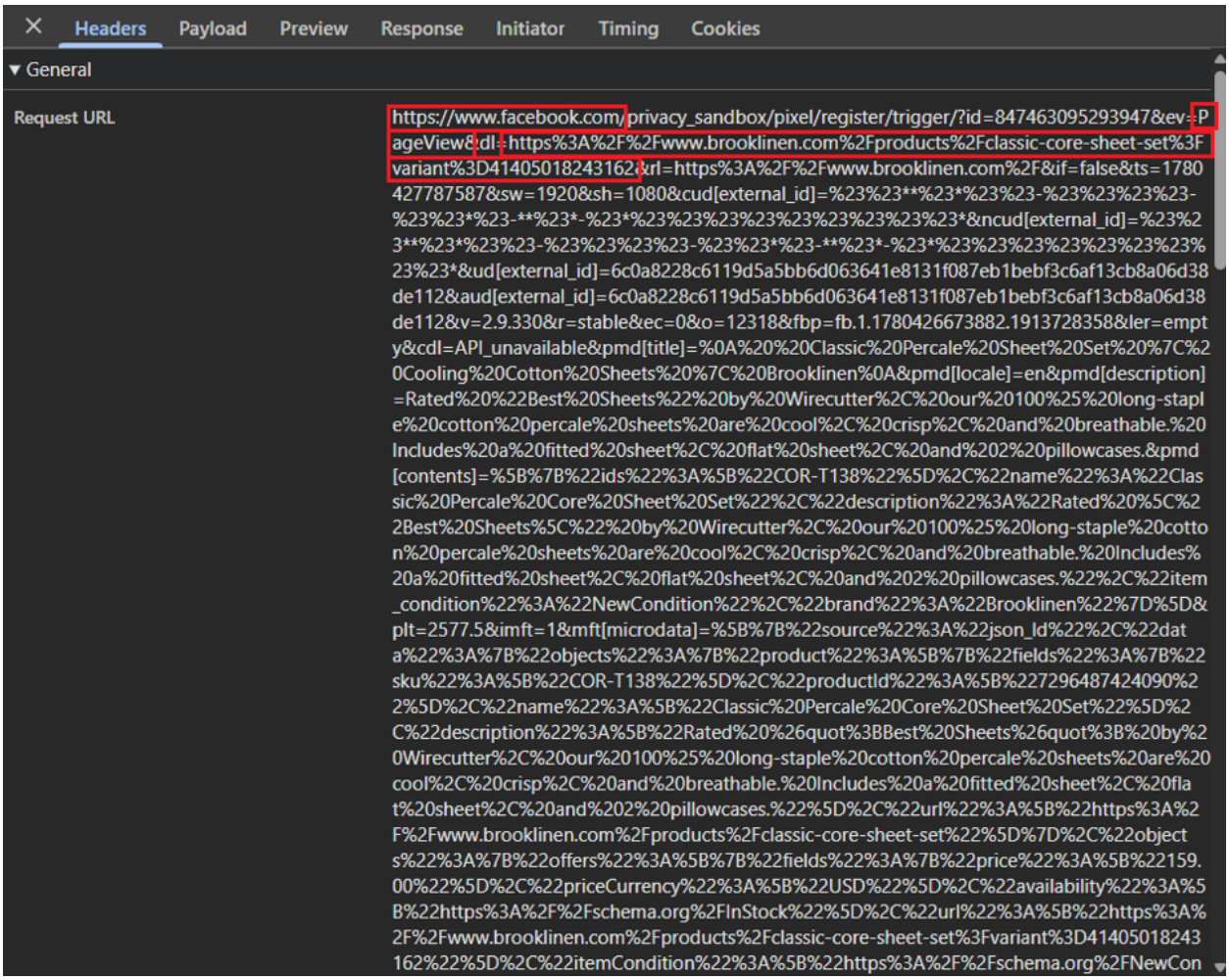


Figure 6 – Request URL of sample webpage from Figure 5, encoded for transmission (compare with decoded URL in Figure 6)

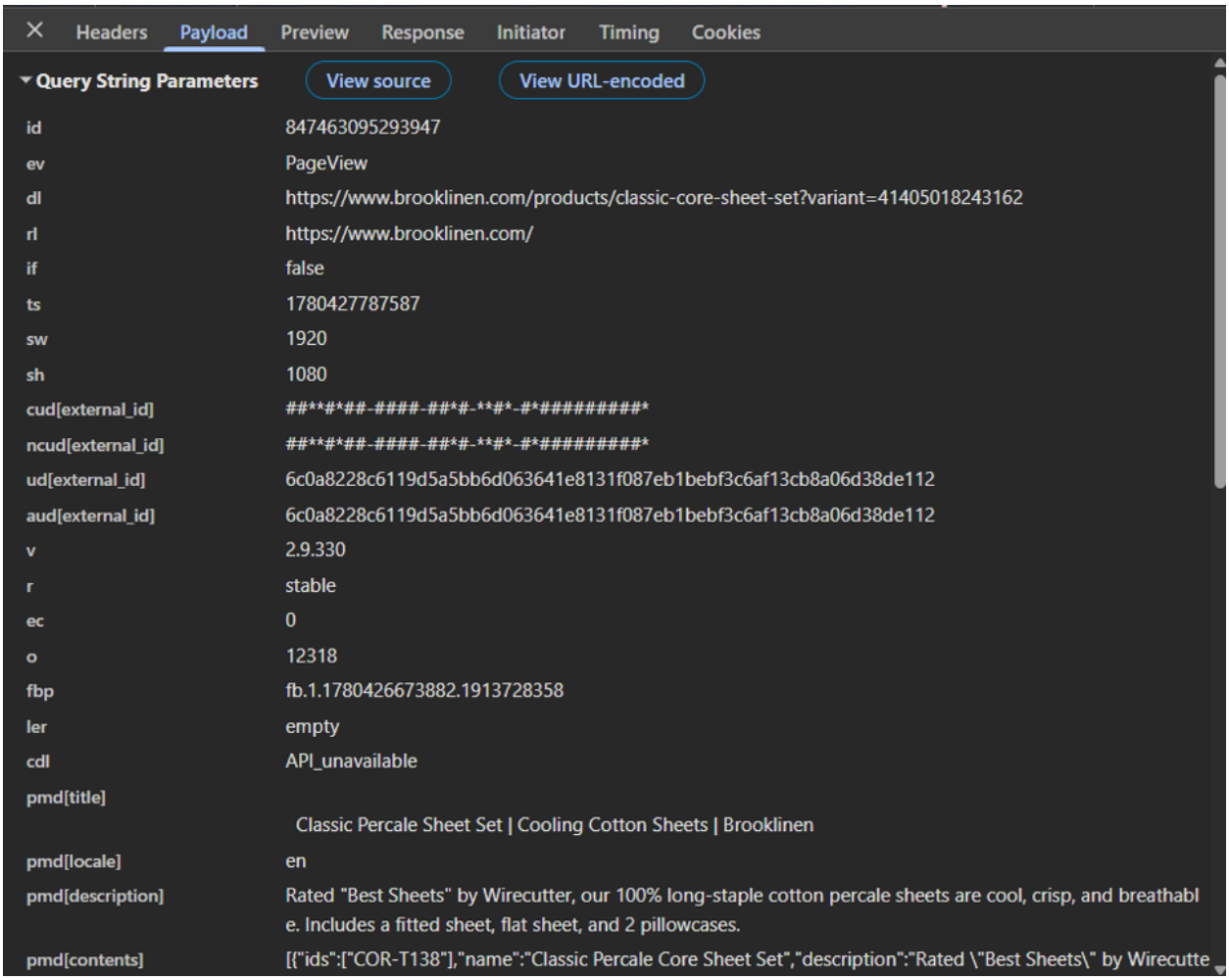


Figure 7 – Decoded, parsed data from Request URL in Figure 6, showing easy-to-read parameters and metadata

32. After sending the Request URL, and after the server responds to the Request URL, the user's browser assembles the packets sent by the server back into the HTML code of the webpage, which is then processed by the user's browser, as it arrives,[15] and rendered into a visual

[15] This processing of webpage data as it arrives is called "parsing," and allows web browsers to convert raw data received over the internet into structured data objects used by the renderer built into the browser to create images on the screen. In short, unless a software command, like a Tracking Tool, is physically last to arrive at a device, it is loaded and executed before the communication has finished being received. *See Populating the page: how browsers work*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Feb. 20, 2026).

display according to the instructions of the HTML code.[16] This is the visible, and usually interactable, website that most people think of.

33. To provide more complex website functionality, website developers will include more complex commands written in other computer programming languages, such as JavaScript snippets, within the HTML documents.[17]

34. Such complex tasks include code used to monitor and report users' activity.

35. In short, the Internet relies on a constant back-and-forth stream of requests and responses between a user's browser and a website's stored coding and data. Importantly, the requests and responses provide a perfect snapshot of everything a user does (or does not do) on a website, and when and how they do it, and with what software and hardware.

36. Unbeknownst to users, as they browse the Website, the Tracking Tools, including third- and first-party cookies, capture and record both incoming and outgoing requests and responses that make up their entire experience on the Website.

II. Defendant Programmed the Website to the Tracking Tools

37. Defendant voluntarily integrated Tracking Tools from at least the Tracking Entities into its Website's programming. Defendant's use of such Tracking Tools on its Website is performed pursuant to commercial agreements between Defendant and third parties, including the Tracking Entities. The Website causes users' devices to store and/or transmit both first-party and third-party tracking cookies. Cookies are small text files sent by a website's server to a user's web browser and stored locally on the user's device. Cookies typically contain unique identifiers that enable a website to recognize and differentiate individual users. These cookie files are

[16] *What Is a URL?*, MOZILLA, *https://developer.mozilla.org/en-us/docs/learn/common_questions/what_is_a_url* (last visited May 7, 2026).

[17] *See JavaScript: Adding interactivity*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/JavaScript_basics (last visited Feb. 17, 2026).

automatically transmitted back to web servers via HTTP requests, allowing the Website and Tracking Entities to identify the device making the request and to record a session reflecting how the user interacts with the Website, i.e., everything they view, click, type, or even hover over.

38. First-party cookies are those placed directly on the user's device by the web server with which the user is knowingly communicating, in this case, Defendant's Website. First-party cookies are commonly used to recognize users across repeated visits to the same website and to track their on-site activity. Third-party cookies are placed by domains other than the Website's domain, such as google.com and other advertising or analytics domains. When a user's browser loads a webpage containing embedded third-party resources, the third party's scripts determine whether its cookies already exist on the user's device and, if not, cause those cookies to be stored. These third-party cookies contain unique identifiers that allow Tracking Entities to recognize and track individual users across different websites, including the Website, and across multiple browsing sessions.

39. As detailed further below, Tracking Tools, including first and third-party cookies, that are placed on users' devices during interactions with the Website are subsequently used to intercept and record users' communications by the Tracking Entities, enabling them to surreptitiously track and collect Website users' Sensitive Information in real time. Tracking Tools serve numerous commercial purposes, including: (i) analytics, such as measuring user engagement and Website performance; (ii) personalization, including remembering users' preferences; (iii) advertising and targeting, including delivering targeted or behavioral advertisements based on users' profiles; and (iv) social media integration.

40. Ultimately, Tracking Tools enable Defendant and Tracking Entities to earn more money and enhance marketing effectiveness through the collection, analysis, and dissemination

of users' Sensitive Information, especially as that Sensitive Information is used to build detailed marketing profiles of users to enhance the effectiveness and efficiency of Tracking Entities' and Defendant's marketing efforts.

41. Importantly, the use of a user's data for marketing purposes occurs whether or not a user actually encounters an ad. In the world of marketing, knowing who to market to is valuable, just as is knowing who not to market to, in the hopes of using marketing budgets efficiently.[18]

42. Defendant owns and operates the Website, which allows users to access information regarding its apparel and headwear products, including caps, clothing, and accessories; browse collections, collaborations, and featured releases; create and manage customer accounts; and purchase merchandise online. When users interact with the Website by navigating pages, clicking links, or entering information, they communicate directly with Defendant. Defendant chooses to place the Tracking Tools on the Website such that, when users visit the Website, both first-party and third-party cookies are placed on users' devices and/or monitored and transmitted to the Tracking Entity associated with each Tracking Tool, along with parameters, metadata, and detailed Request URLs. Because Defendant controls the Website's software code and determines which Tracking Tools are loaded onto users' browsers, Defendant has control over whether these Tracking Tools are placed and whether users' Sensitive Information is transmitted to Tracking Entities.

43. Defendant's explanation as to its use of Tracking Tools on the Website is contained in its Privacy Policy[19]:

---

[18] *See* Kyle Morehouse, *Increase Ad ROI With Audience Suppression*, ADOBE (Jan. 24, 2017) (https://blog.adobe.com/en/publish/2017/01/24/increase-ad-roi-audience-suppression) (last visited June 4, 2026) (discussing a fundamental digital marketing practice called "audience suppression" that utilizes tracking data to identify individuals who should not receive further ads).

[19] *Brooklinen's Privacy Policy*, BROOKLINEN (last updated Jan. 21, 2026) https://www.brooklinen.com/pages/privacy (last viewed June 18, 2026).

> When you visit, use or navigate the Site, we automatically collect certain information about your device, including information about your web browser, IP address, time zone, location, and some of the cookies that are installed on your device. Additionally, as you browse the Site, we collect information about the individual web pages or products that you view, what websites or search terms referred you to the Site, and information about how you interact with the Site. We refer to this automatically-collected information as "Device Information.
>
> The Privacy Policy further states:
>
> Third-Party Data Partners and Advertising - When you visit or log in to our Site, cookies and similar technologies may be used by our online data partners or vendors to associate these activities with other personal information they or others have about you, including by association with your email or home address. We (or service providers on our behalf) may then send communications and marketing to these email or home addresses.

44. The Cookie Settings explain different categories of cookies. It represents that "Strictly Necessary Cookies" are used for the Website to enable basic website functionality:

> **Strictly Necessary Cookies**
>
> These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.

45. The Cookie Settings further represent that "Targeting Cookies" cookies are set by advertising partners and used to build user profiles:

> **Targeting Cookies**
>
> These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

46. The Cookie Settings further represent that "Performance Cookies" cookies are used to p count visits and traffic sources:

> **Performance Cookies**
>
> These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

47. Defendant's Cookie Banner and Cookie Settings clearly inform users that their detailed browsing activity and interactions with the Website would ***not*** be captured and transmitted to Tracking Entities via Tracking Tools through the use of cookies when users affirmatively reject the use of non-necessary cookies.

III. The Website's Cookie Banner and Cookie Settings Misled Users

48. When visiting the Website, the Website immediately displayed a Cookie Banner that stated:

> We use cookies to make your browsing experience feel as smooth and comfortable as our sheets. By continuing, you agree to our use of cookies. You can adjust your preferences anytime. Further information is available in our Cookie Policy.[20]

49. The Cookie Banner presented users with options to "Manage Preferences" and "Accept Cookies," as well as a hyperlink to Defendant's Cookie Policy. Users were also provided

[20] *See Figures 1* and *8*, which depict Defendant's Cookie Banner and Cookie Settings.

with a close ("X") button to dismiss the Cookie Banner. Upon selecting "Accept Cookies" or dismissing the Cookie Banner, the banner disappeared from view.

50. Website users who selected the "Manage Preferences" option were presented with the Cookie Settings, which represented that users could control how their Sensitive Information was collected and shared by accepting only essential cookies. These Cookie Settings are implemented through the Website's consent-management framework, which operates in conjunction with the scripts and technologies used to manage the Website's third-party Tracking Tools.

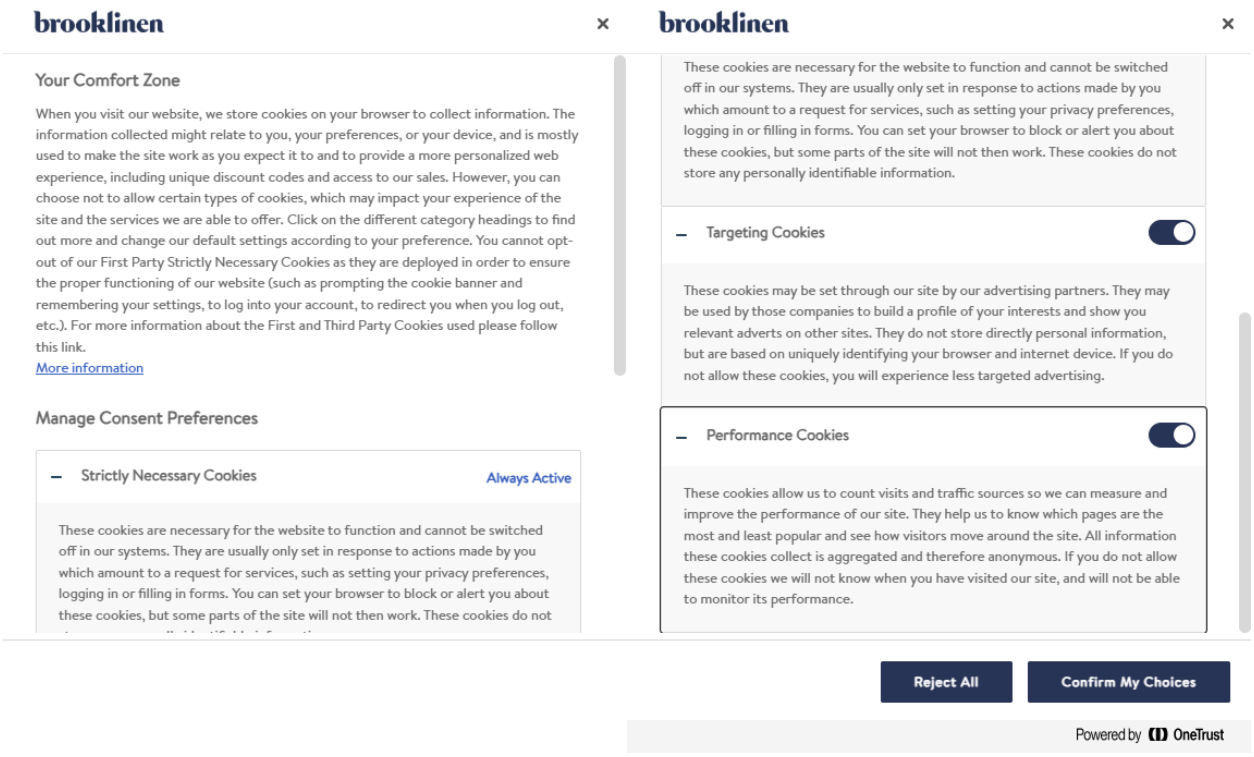


Figure 8 – Brooklinen's Cookie Settings, representing that users can manage the use of cookies

51. After users made their choices and clicked the "Confirm My Choices" button, the Cookie Settings window disappeared.

52. The representations made by Defendant in the Cookie Banner and Cookie Settings led Plaintiff, and would reasonably lead all Website users similarly situated, to believe that they

had successfully disabled all but necessary cookies via their express rejection. The Cookie Banner and Cookie Settings further reasonably led Plaintiff and all reasonable users to believe that Defendant would not allow Tracking Entities, through cookies, to access users' Sensitive Information. Plaintiff acted on those representations by interacting with the Website after making privacy selections intended to reject any sharing of her personal information and use of any Tracking Tools other than necessary cookies.

53. These representations were false. Defendant did not abide by Plaintiff's expressed preferences and does not abide by users' expressed preferences. When users choose to reject all non-essential cookies, they clearly communicate that they do not consent to the placement or transmission of Tracking Tools using cookies other than those required for functionality. Nevertheless, Defendant continued to cause the Tracking Tools and their associated cookies to be placed or otherwise accessed on users' browsers and devices so that Tracking Entities could intercept, transmit, and use users' Sensitive Information in real time.

54. The Tracking Tools that Defendant caused to be loaded and executed by users' browsers function as an unlawful wiretap, pen register, and trap and trace device when executed because they enable Tracking Entities, separate and distinct parties from Defendant, to eavesdrop on, record, extract, analyze, and exploit users' Sensitive Information. The Tracking Entities are not mere passive tools or instruments of the Defendant; they collect, analyze, and use the intercepted communications for their independent monetary gain.

IV. Defendant's Website Procured Tracking Entities to Spy on Users

55. Defendant operates the Website and has installed Tracking Tools on the Website created by Tracking Entities. These Tracking Tools operate invisibly, tracking Website users' activity by intercepting users' Sensitive Information as it arrives at or is sent from users' devices,

copying the contents of those communications, and generating new Request URLs containing portions of the copied communications, which are transmitted to the Tracking Entities. Generally, the Tracking Tools collect information about users' activity on the Website when events specified by Defendant, such as loading specific webpages, clicking links, or submitting information, are monitored by the Tracking Tools. Defendant adds parameters to these events, enhancing the scope and specificity of the collected data. Parameters are strings of text that website owners add to a URL to track and organize their webpages.[21]

56. URL parameters include key-value pairs formatted as "key=value."

a. The "key" is what the website owner wants to adjust or track (e.g., "color" or "ev" for event)

b. The "value" is the specific setting or data for that parameter (e.g., "yellow" or "AddToCart" for a user taking the action of adding a product to their online shopping cart)

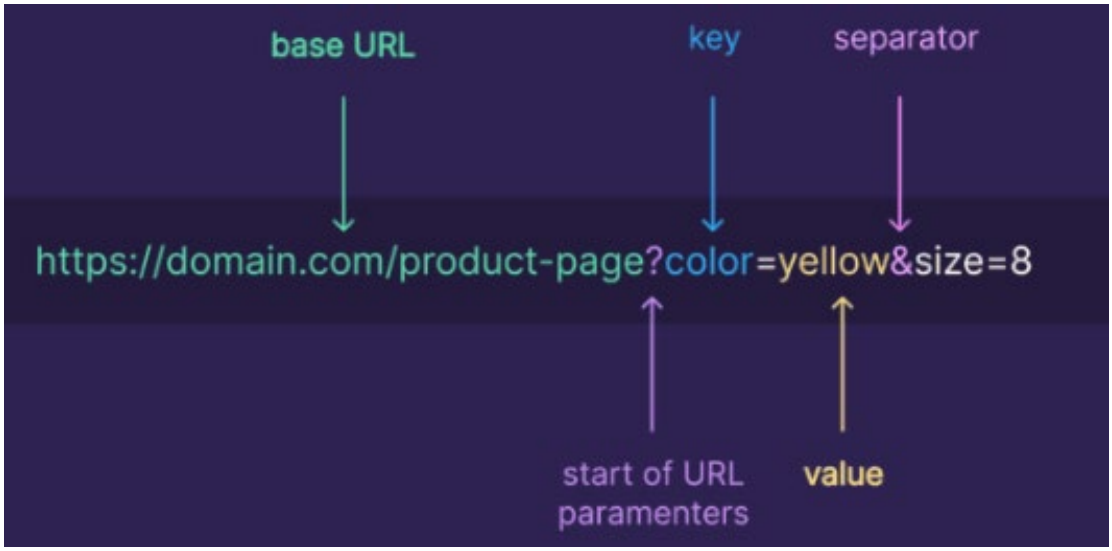


Figure 9 – Diagram of a URL displaying how parameters function[22]

[21] Yongi Barnard, *URL Parameters: What They Are and How to Use Them Properly*, BACKLINKO (last updated Feb. 5, 2026), https://backlinko.com/url-parameters (last visited May 7, 2026).
[22] *Id.*

A. The TikTok Pixel

57. TikTok offers software known as a "tracking pixel" to track users' actions, behavior, and conversions across the Website (the "TikTok Pixel").

58. The TikTok Pixel is a snippet of code that begins to collect information the moment a user lands on the Website, before any pop-up or cookie banner advises them of the invasion or seeks their consent. To use the TikTok Pixel, the website operators, including Defendant, must include the specific pixel IDs associated with their websites, which allows TikTok to link the intercepted data back to their individual TikTok business profiles.[23]

59. Defendant's TikTok Pixel ID is included in transmissions sent to and from users' devices, as seen in *Figures 12* and *15*—the TikTok JavaScript code in *Figure 12* references Defendant's Pixel ID, whereas the "code" variable in *Figure 15* identifies the TikTok Pixel ID, both of which reference the Pixel ID as "C7SQCJOFLK2NRAISUAC0".

60. TikTok Pixel users make use of events to collect even more specific data on users' activities, including for the actions taken on a webpage (e.g., clicking a specific button or element, adding an item to a cart, and when a webpage with a URL containing a specified keyword is loaded onto a user's browser), the value of the purchase, and the product purchased.[24]

61. These event-triggers cause data to be sent as communications are received by users (through webpage loading events), and as communications are sent to the Website (through button clicking and similar events).

62. The TikTok Pixel also collects:

---

[23] *See generally Troubleshoot with Pixel Helper*, TIKTOK, https://ads.tiktok.com/help/article/tiktok-pixel-helper-2.0?lang=en (last visited Feb. 17, 2026) (noting that a missing or invalid Pixel ID will cause errors when using the TikTok Pixel).

[24] *How to Set Up Events and Parameters with Events Builder*, TIKTOK, https://ads.tiktok.com/help/article/how-to-set-up-events-and-parameters (last visited Feb. 17, 2026) (describing how to designate events).

a. The time website actions took place;

b. The IP address (which is used to determine the geographic location of a user);

c. Device information, including make, model, operating system, and browser information;

d. Cookies that can be used to identify users; and

e. Metadata and button clicks.[25]

63. The information the TikTok Pixel collects provides Defendant and TikTok with a better understanding of who Defendant's customers are, which webpages users have visited, and how they interact with the Website.

64. TikTok's "Advanced Matching" feature allows Defendant to "match customer information such as email and phone number along with actions people take on [the Website]."[26] Once Advanced Matching is active, the TikTok Pixel "will automatically find customer information and match it with people on TikTok."[27] TikTok then provides Defendant with custom audiences based on website user events, like page views or purchases, to model lookalike audiences.[28] Lookalike audiences allow Defendant to retarget users who have already visited or made purchases on the Website and serve them relevant ads on TikTok based on their interactions with the Website.[29]

---

[25] *About TikTok Pixel*, TIKTOK, https://ads.tiktok.com/help/article/tiktok-pixel (last visited Feb. 17, 2026).
[26] *About Advanced Matching for Web*, TIKTOK, https://ads.tiktok.com/help/article/advanced-matching-web?lang=en (last visited Feb. 17, 2026).
[27] *How to set up Automatic Advanced Matching*, TIKTOK, https://ads.tiktok.com/help/article/how-to-set-up-automatic-advanced-matching?lang=en (last visited Feb. 17, 2026).
[28] *Get started with the TikTok Pixel: a small business guide*, TIKTOK (Sept. 6, 2024) https://ads.tiktok.com/business/en-US/blog/get-started-with-tiktok-pixel (last visited Feb. 17, 2026) (benefits of using the TikTok Pixel).
[29] *See* Lizzie Davey, *How to use TikTok Pixel: TikTok conversions tracking*, LEADSBRIDGE (May 2, 2025) https://leadsbridge.com/blog/tiktok-pixel/ (last visited Feb. 17, 2026).

65. Put simply, the TikTok Pixel collects as much data as it can about otherwise anonymous visitors to the Website and matches it with existing data TikTok has acquired and accumulated about hundreds of millions of Americans to identify users and develop their marketing profiles, improving Defendant's conversion rates and reducing overall advertising costs.[30]

66. Defendant used the TikTok Pixel to monitor and log, in real time from users' browsers, when users clicked on specific products, loaded webpages, added specific products to cart, and proceeded through the checkout process to payment and shipping.

67. The TikTok Pixel also captures users' identifying cookies (the _ttp cookie is used to identify TikTok users[31]).

68. Plaintiff had a reasonable expectation that the following information would not be exposed to the Tracking Tools placed by Defendant: (i) Plaintiff' identifying information, (ii) information that designated Plaintiff as interested in purchasing or otherwise as a purchaser of the Defendant's products, and (iii) IP address and identifier information relating to who Plaintiff is, and who Plaintiff was communicating with to obtain the products.

69. Using the TikTok Pixel benefits Defendant by allowing Defendant to effectively track conversions, optimize the delivery of its ad campaigns, create and target its own custom audiences, and create and access vast amounts of data to run successful ad campaigns.[32]

---

[30] *Id.*

[31] *See G-Star Raw: List of Cookies* https://assets.g-star.com/v1/static/Cookielist_Jun_2022#:~:text=Tiktok%20tta_attr_id.%2012%20months%20This%20cookie%20is,measure%20how%20different%20campaigns%20and%20marketing%20strategies (last visited Feb. 17, 2026).

[32] *See Benefits of using the TikTok Pixel*, TIKTOK (Sept. 6, 2024) https://ads.tiktok.com/business/en-US/blog/get-started-with-tiktok-pixel?acq_banner_version=73412989 (last visited Feb. 17, 2026).

70. TikTok benefits, in turn, by using data collected by the TikTok Pixel to improve its own products and services, including the sale of targeted advertising, and to generate its own benchmarking reports to share with other TikTok business customers.[33]

71. In fact, TikTok admits that it gathers Website visitors' Sensitive Information via the TikTok Pixel and shares that Sensitive Information with third or fourth parties,[34] just as Plaintiff's Sensitive Information was gathered and shared here.

72. According to a leading data security firm, the TikTok Pixel secretly installed on Defendant's Website is particularly invasive. The TikTok Pixel "immediately links to data harvesting platforms that pick off usernames and passwords, credit card and banking information, and details about users' personal health."[35] The TikTok Pixel also collects "names, passwords and authentication codes" and "transfer[s] the data to locations around the globe," and does so "before users have a chance to accept cookies or otherwise grant consent."[36]

73. An image of the invasive TikTok code secretly embedded on Defendant's Website can be seen here, which shows the Website instantly sending communications to TikTok to add to its collection of user behavior:

[33] *TikTok Business Products (Data) Terms*, TIKTOK (July 29, 2024) http://ads.tiktok.com/i18n/official/policy/business-products-terms (last visited Dec. 22, 2025).
[34] *See Privacy Policy*, TIKTOK (Feb. 5, 2026) https://www.tiktok.com/legal/page/us/privacy-policy/en (last visited Feb. 26, 2026).
[35] *See* Aaron Katersky, *TikTok Has Your Data Even If You've Never Used The App: Report*, ABC NEWS (Mar. 16, 2023 1:59 PM), https://abcnews.go.com/Business/tiktok-data-app-report/story?id=97913249 (last visited Feb. 17, 2026).
[36] *Id.*

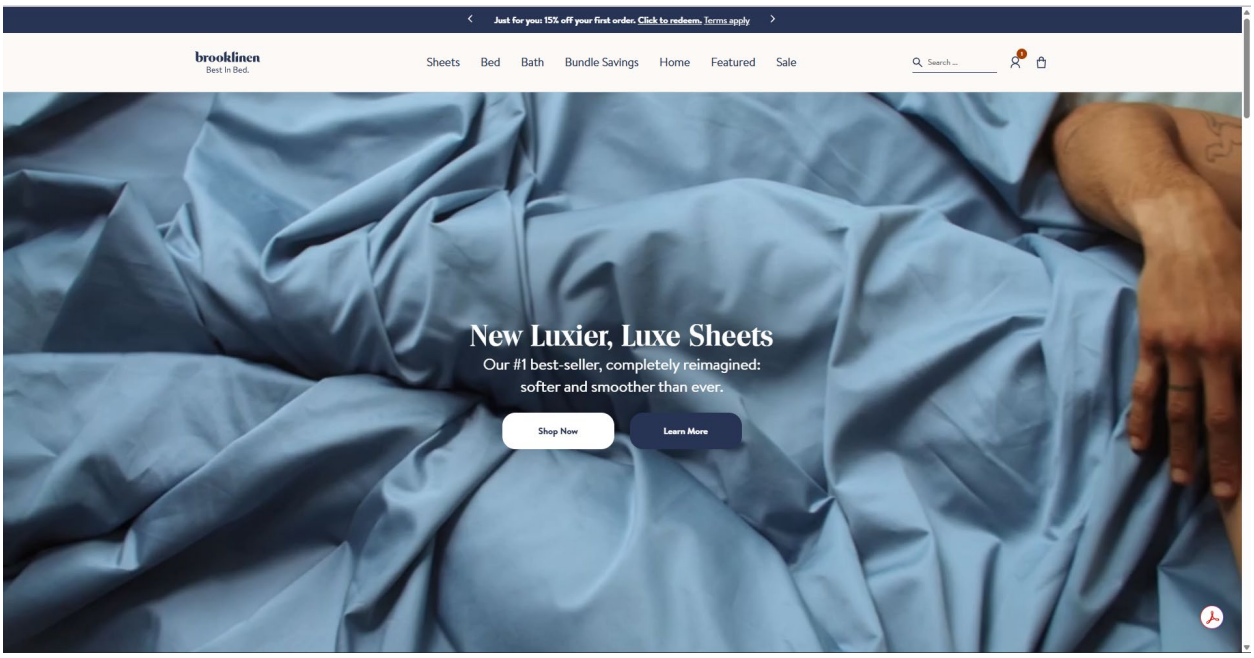


Figure 10 – Home page of the Website

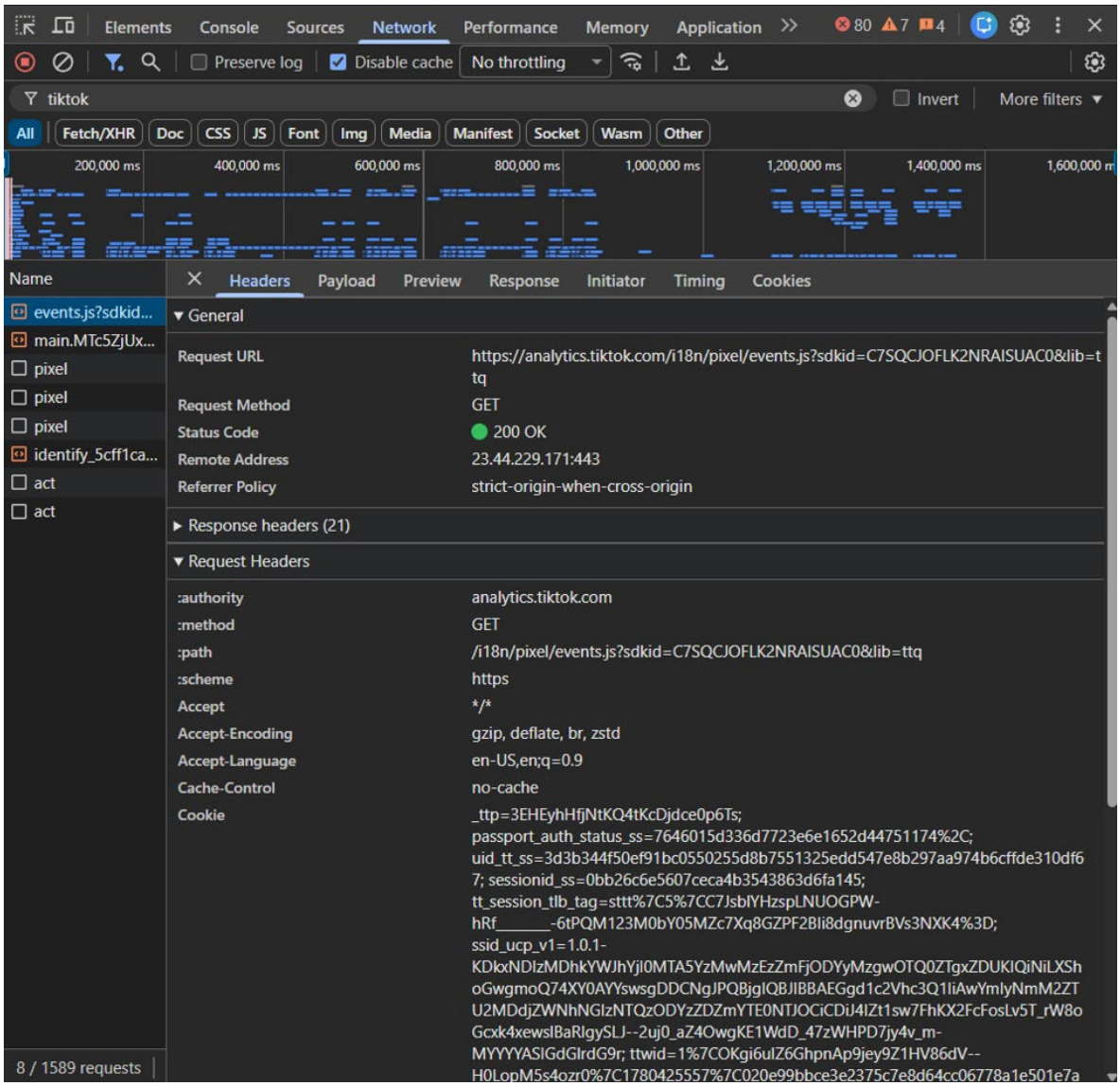


Figure 11 – Using a browser's "developer tools" while visiting Brooklinen's webpage confirms the Website loading TikTok Pixel's code onto the user's browser, which caused the transmission of an HTTP Request to TikTok's servers

Figure 12 – Defendant's TikTok Pixel code on the Website displaying the active features of the TikTok Pixel on the Website, including Advanced Matching and AutoAdvancedMatching

74. The TikTok Pixel instantly sends communications to TikTok when a user views the page and tracks page interactions. The screenshots below show the sample webpage along with the webpage code, including the various TikTok scripts Defendant causes to run on users' browsers, and the electronic impulses sent to TikTok from users' browsers to aid TikTok's building of marketing profiles on users:

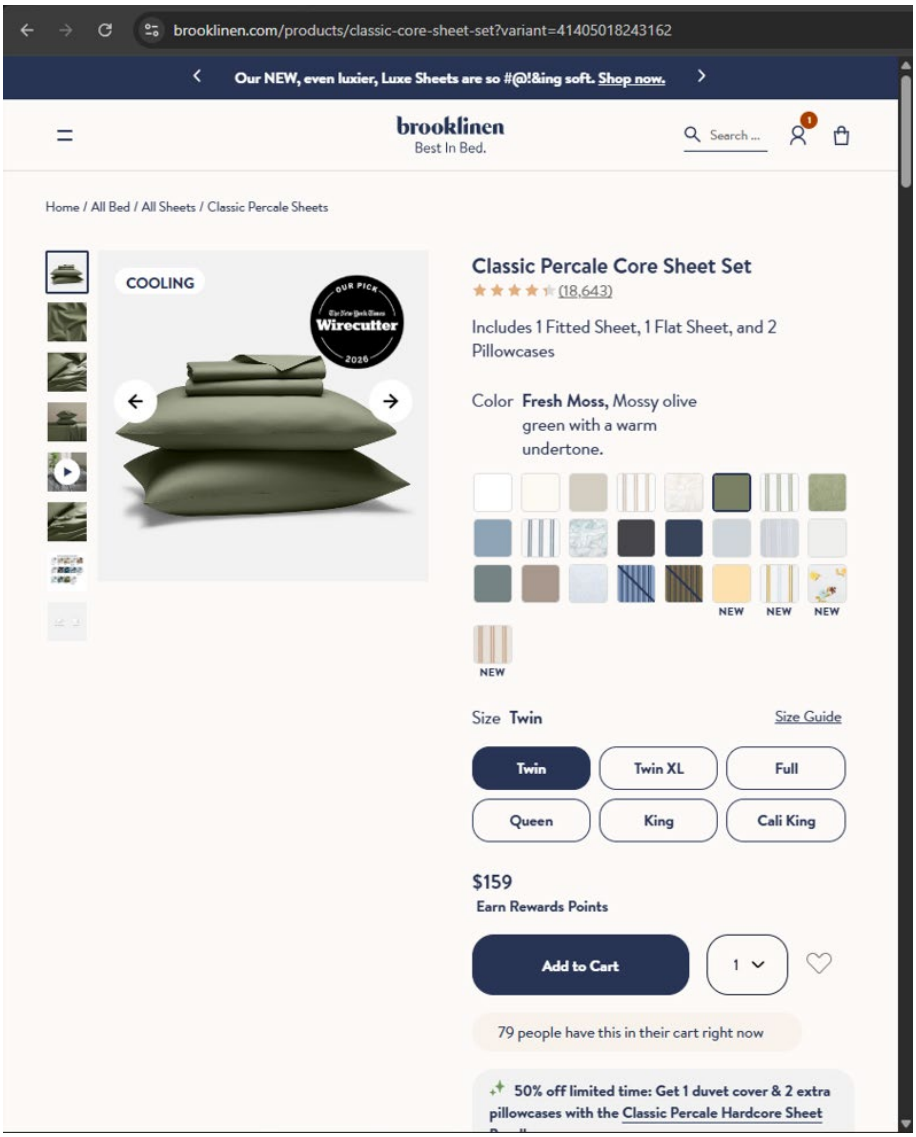


Figure 13 – Sample product on the Website

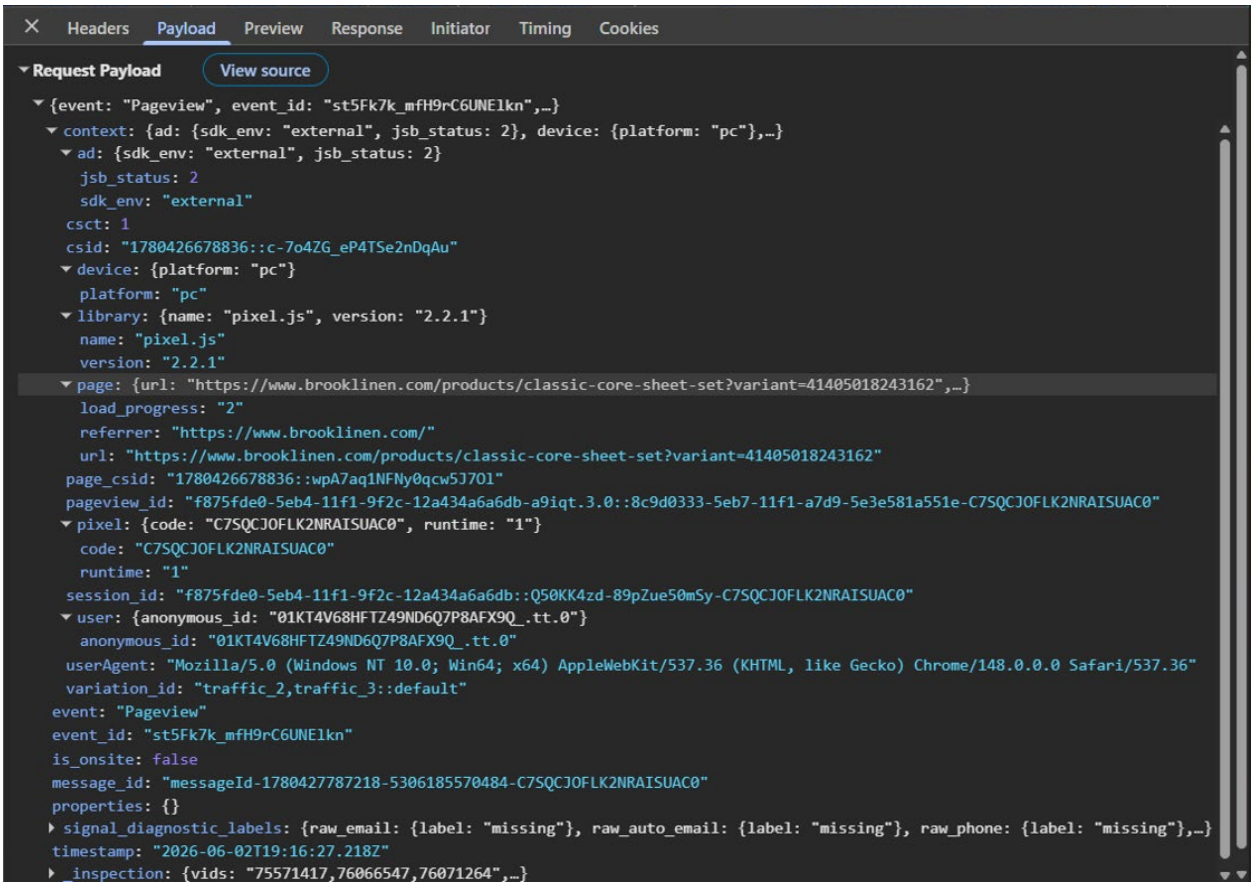
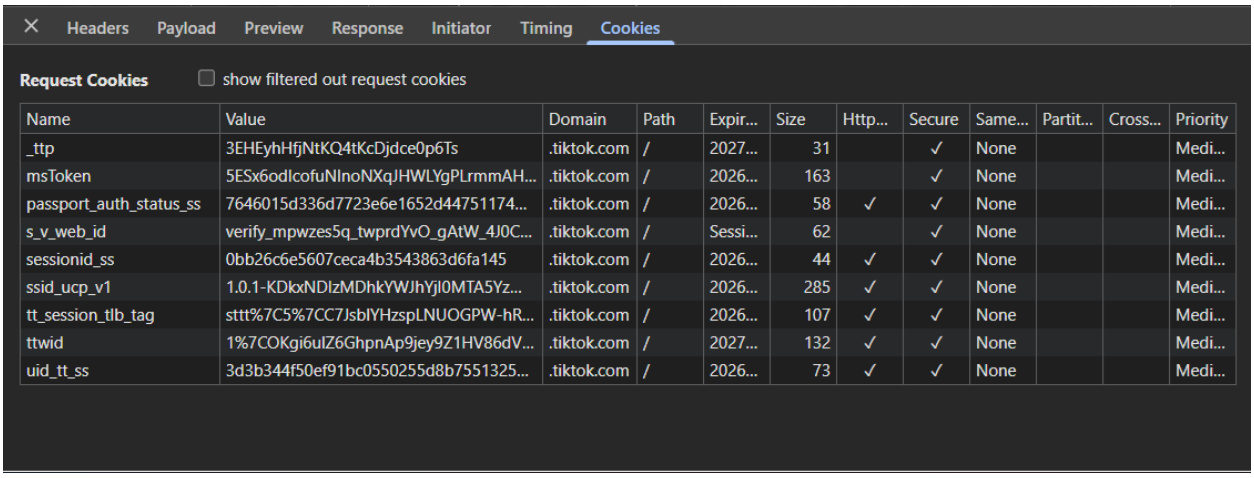


Figure 14 – Information collected via the TikTok Pixel when a user visits the sample webpage from Figure 13



Name	Value	Domain	Path	Expir...	Size	Http...	Secure	Same...	Partit...	Cross...	Priority
_ttp	3EHEyhHfjNtKQ4tKcDjdce0p6Ts	.tiktok.com	/	2027...	31		✓	None			Medi...
msToken	5ESx6odIcofuNInoNXqJHWLYgPLrmmAH...	.tiktok.com	/	2026...	163		✓	None			Medi...
passport_auth_status_ss	7646015d336d7723e6e1652d44751174...	.tiktok.com	/	2026...	58	✓	✓	None			Medi...
s_v_web_id	verify_mpwzes5q_twprdYvO_gAtW_4J0C...	.tiktok.com	/	Sessi...	62		✓	None			Medi...
sessionid_ss	0bb26c6e5607ceca4b3543863d6fa145	.tiktok.com	/	2026...	44	✓	✓	None			Medi...
ssid_ucp_v1	1.0.1-KDkxNDIzMDhkYWJhYjI0MTA5Yz...	.tiktok.com	/	2026...	285	✓	✓	None			Medi...
tt_session_tlb_tag	sttt%7C5%7CC7JsbIYHzspLNUOGPW-hR...	.tiktok.com	/	2026...	107	✓	✓	None			Medi...
ttwid	1%7COKgi6uIZ6GhpnAp9jey9Z1HV86dV...	.tiktok.com	/	2027...	132	✓	✓	None			Medi...
uid_tt_ss	3d3b344f50ef91bc0550255d8b7551325...	.tiktok.com	/	2026...	73	✓	✓	None			Medi...

Figure 15 – Cookies transmitted TikTok Pixel on the Website

75. To use the TikTok Pixel, Defendant agreed to TikTok's Business Products (Data) Terms (the "TikTok Terms"). But Plaintiff and other Website visitors are never exposed to these

terms (nor would they have any reason to look for them), as they form the agreement between Defendant and TikTok, which agreement is not even known to Plaintiff or Website visitors.

76. The TikTok Terms inform website owners using TikTok Pixel that their use of the TikTok Pixel shares or enables TikTok to access their website users' contact details, developer data, and/or event data.[37]

77. The TikTok Terms are transparent that TikTok will process users' data to match contact details against corresponding accounts and subsequently match those accounts with the users' corresponding event data.[38]

78. TikTok puts TikTok Pixel users, such as Defendant, on notice that they "must only share with us or enable us to access Business Products Data in a manner that is transparent and lawful."[39] TikTok makes clear that the onus is on the Defendant to provide all necessary transparency notices and obtain all necessary rights, permissions, and lawful bases, including consent, to share information with TikTok.

79. TikTok educates and reminds TikTok Pixel users of their obligation not to share any data "from or about Children or that includes health or financial information, or other categories of sensitive information."[40]

80. As a sophisticated party entering into a business arrangement with another sophisticated party, Defendant was on notice of the potential privacy violations that would result from use of the TikTok Pixel and ignored TikTok's warnings to safely handle its users' data and warn their users that the Website would disclose their information in a manner that threatened their private information.

---

[37] *TikTok Business Products (Data) Terms*, TIKTOK (July 29, 2024), (last visited Dec. 22, 2025).
[38] *Id.*
[39] *Id.*
[40] *Id.*

B. The Meta Pixel

81. Facebook offers its own tracking pixel known as the Facebook or Meta Pixel (the "Meta Pixel") to website owners for the purpose of monitoring user interactions on their websites, which can then be shared with Facebook.

82. The Meta Pixel is a marketing tool that can only be added to a webpage by website developers. A website operator must sign up for a business account or link a related Facebook account to its Pixel, then add code to the website to use the Meta Pixel.[41]

83. Upon creating a Meta Pixel, a Pixel ID (also called a DataSet ID by Meta) is generated.[42] This Pixel ID is used to initialize the Meta Pixel, either by allowing Meta to fetch a predetermined library of code associated with that ID or by identifying the website owner's Facebook account used to receive the collected data when programming the Pixel directly into a website.[43]

84. This Pixel ID must match "a known Pixel ID" in Meta's system,[44] and is transmitted by the Meta Pixel.[45]

85. As Facebook notes, the Meta Pixel must be added to each individual page that a website owner wishes to track.[46]

---

[41] *Setup and install the Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited Feb. 17, 2026).
[42] *Id.*
[43] *Get Started*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/get-started/ (last visited Feb. 17, 2026) ("To install the Pixel, add its base code . . . on every page where you will be tracking website visitor actions.").
[44] *Pixel Helper*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/support/pixel-helper (last visited Feb. 17, 2026).
[45] *Meta Pixel*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/ (last visited Feb. 17, 2026).
[46] *Get Started*, FACEBOOK, (last visited Feb. 17, 2026) ("To install the Pixel, add its base code . . . on every page where you will be tracking website visitor actions.").

86. Defendant places the Meta Pixel on the Website to gather, collect, and then transmit user information to Facebook.[47] Defendant and Facebook use this information to build valuable personal profiles for Website users to inform their targeted advertising campaigns, enhancing marketing effectiveness and increasing the chance of converting users into paying customers.[48]

87. The harvested data improves Defendant's advertising by pinpointing audience demographics by interests, gender, or location, and finding the people who are most likely to take action and view content.[49]

88. Once implemented on a website, the Facebook Pixel begins to share users' information the moment a user lands on the website.

89. When a Facebook user logs onto Facebook, tracking cookies, including the "c_user" cookie, the datr cookie, and the "fr" cookie, are automatically created and stored on the user's device.[50] These cookies allow Facebook to link the data it receives through the Meta Pixel to individual Facebook users.

90. The c_user cookie, for example, contains a series of numbers (the user's Facebook ID, or "FID") to identify a user's profile.

Figure 16 – Sample c_user cookie, containing FID of test account created by Plaintiff's counsel to investigate the Facebook Pixel

[47] The Facebook Pixel allows websites to track visitor activity by monitoring user actions ("events") that websites want tracked and share a tracked user's data with Facebook. *See Meta Pixel*, FACEBOOK (last visited Feb. 17, 2026).
[48] *See Meta Pixel*, FACEBOOK (last visited Feb. 17, 2026).
[49] *See Audience ad targeting*, FACEBOOK, https://www.facebook.com/business/ads/ad-targeting (last visited Feb. 17, 2026).
[50] *Cookies Policy: What are cookies, and what does this* policy cover?, FACEBOOK (Dec. 12, 2023), https://www.facebook.com/policy/cookies/ (last visited Feb. 17, 2026).

91. The FID can simply be appended to www.facebook.com/ to navigate to the user's profile (e.g., www.facebook.com/[FID]). Appending the FID from *Figure 18* to the Facebook URL in a standard internet browser (here, www.facebook.com/100091959850832) redirects the webpage straight to the Facebook profile associated with the UID, as depicted below:

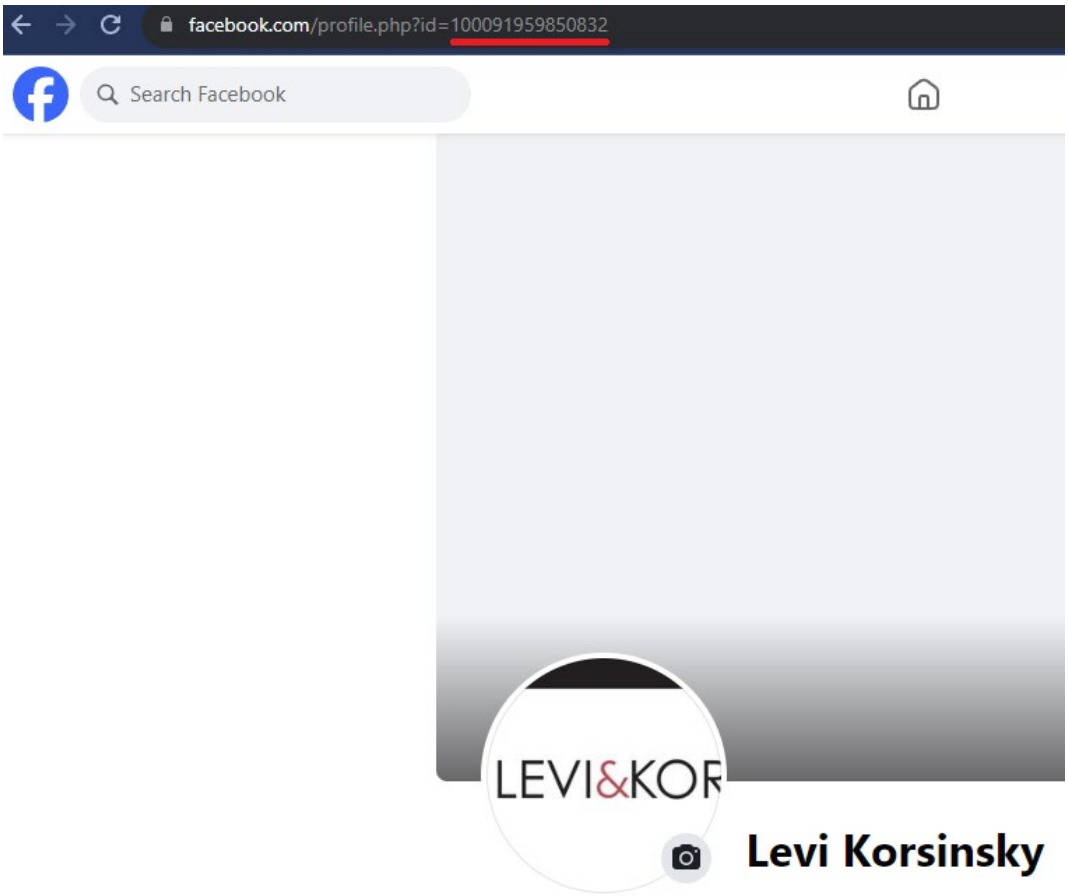


Figure 17 – Sample Facebook account created by Plaintiff's counsel to investigate the Facebook Pixel, with FID highlighted in URL

92. The Meta Pixel tracks user activity on web pages by monitoring events,[51] which, when triggered, cause the Pixel to automatically send users' Sensitive Information directly to

[51] *About Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Feb. 17, 2026).

Facebook.[52] Examples of events utilized by websites include a user loading a page with a Pixel installed (the "PageView event").[53] The Website utilizes this PageView event.[54]

93. The Meta Pixel also transmits Defendant's unique Pixel ID via the "id" parameter, which contains Defendant's Pixel ID of "847463095293947" for the purpose of matching the harvested data to Defendant's Website.

94. Defendant uses the Meta Pixel to monetize Website users' Sensitive Information.

95. Facebook independently benefits from the data collected through the Meta Pixel by using the harvested data to sell targeted advertising services. Facebook benefits from intercepting and analyzing users' Sensitive Information by refining its marketing algorithms and improving the effectiveness of its ad sales to all advertisers through Meta's social media platforms, enabling it to target Meta's users more accurately and profit from the ability to target potential customers more effectively.

96. Meta admits that it shares users' Sensitive Information with third and fourth parties,[55] just as Plaintiff's Sensitive Information was shared here.

97. Defendant's use of the Facebook Pixel on the Website is demonstrated by the screenshots below, which follow a user on the Website.

---

[52] *Id.*

[53] *Specifications for Meta Pixel standard events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Feb. 17, 2026).

[54] The presence of Pixel events can be confirmed by using the publicly available and free Meta Pixel Helper tool. *See About the Meta Pixel Helper*, FACEBOOK, https://www.facebook.com/business/help/198406697184603?id=1205376682832142 (last visited Feb. 17, 2026).

[55] *See Privacy Policy,* META (Dec. 16, 2025), https://www.facebook.com/privacy/policy?section_id=4-HowDoWeShare (last visited Feb. 26, 2026).

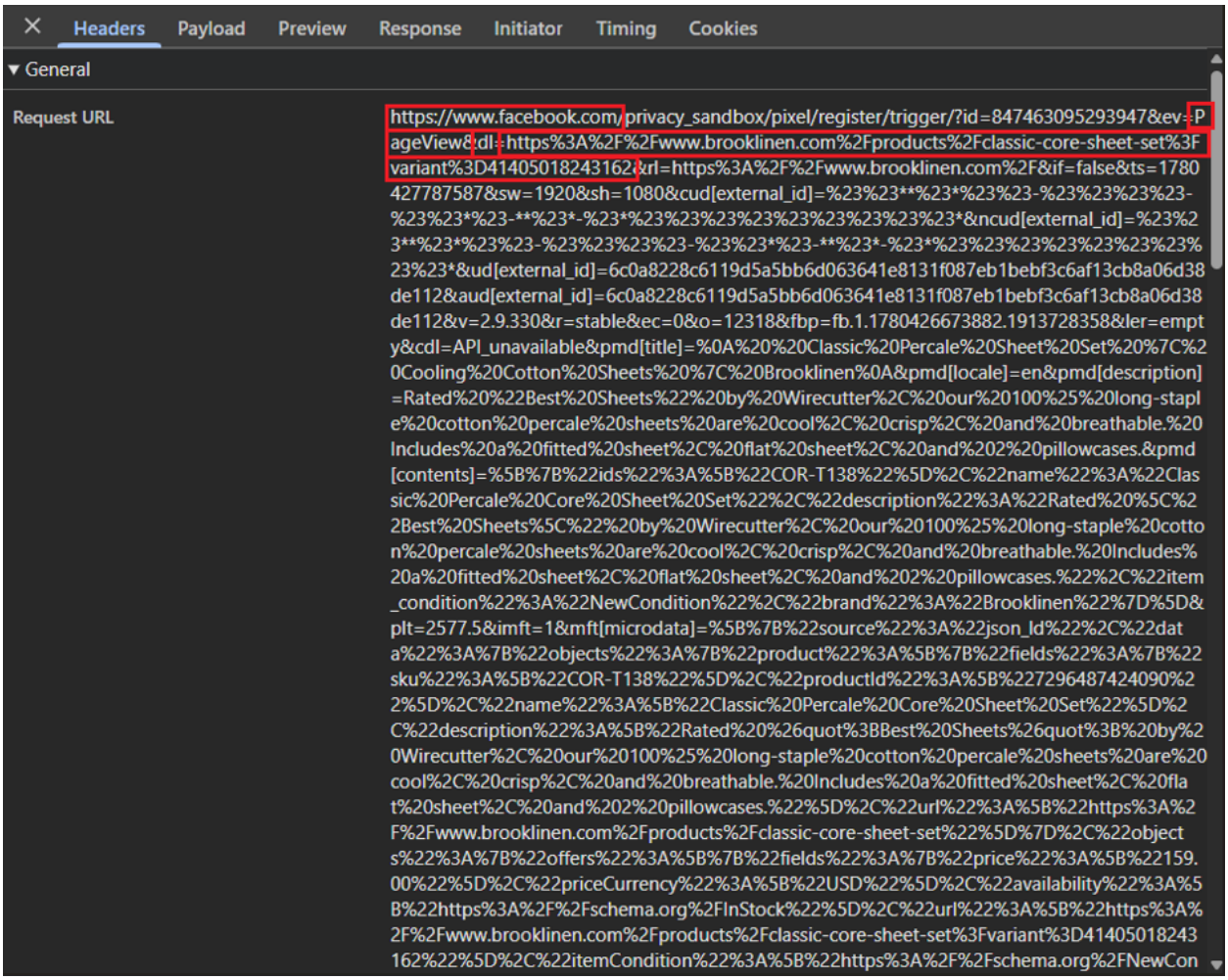


Figure 18 – Facebook Pixel tracking a user on the Website through the "PageView" event

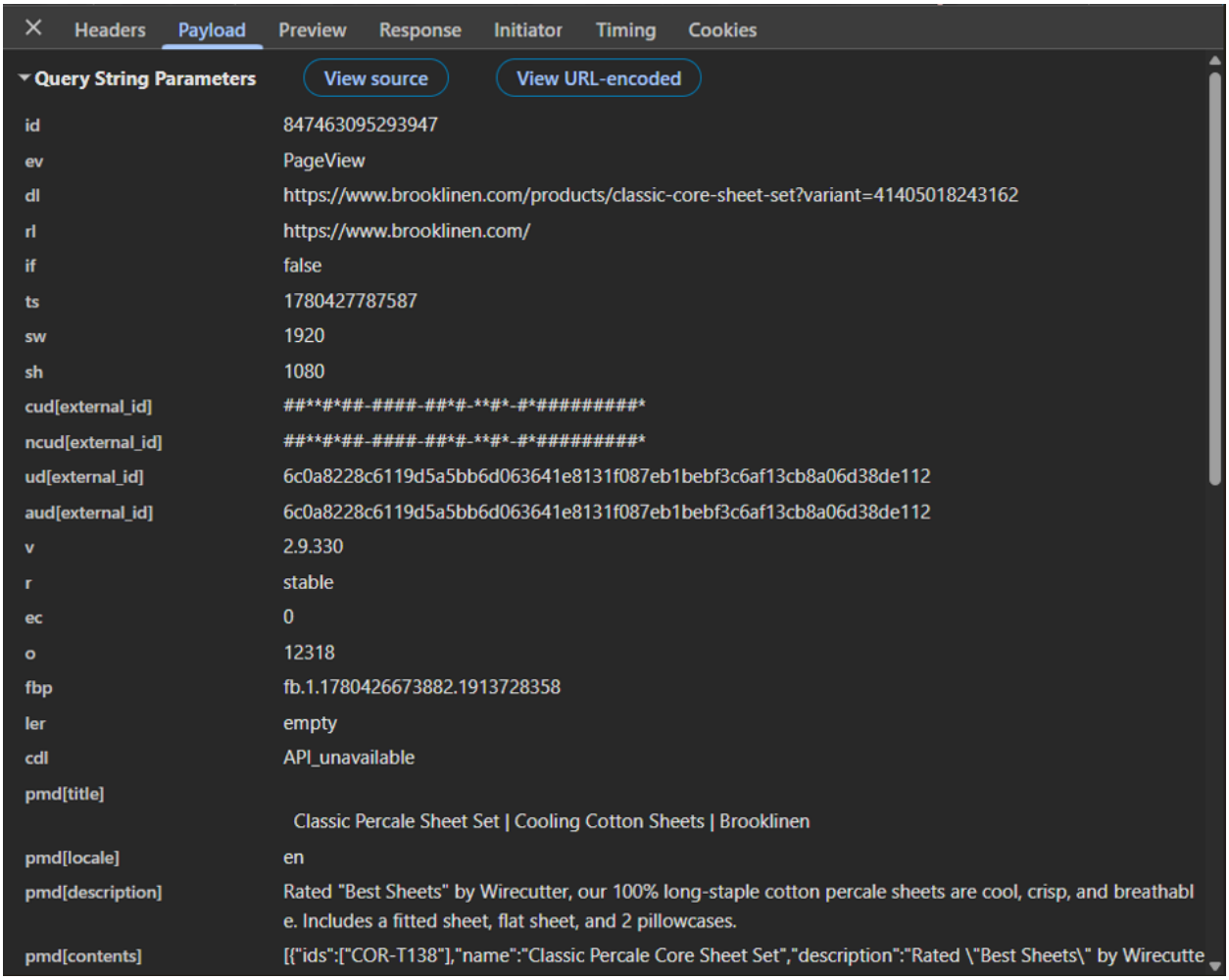


Figure 19 – Information intercepted by the Facebook "PageView" event

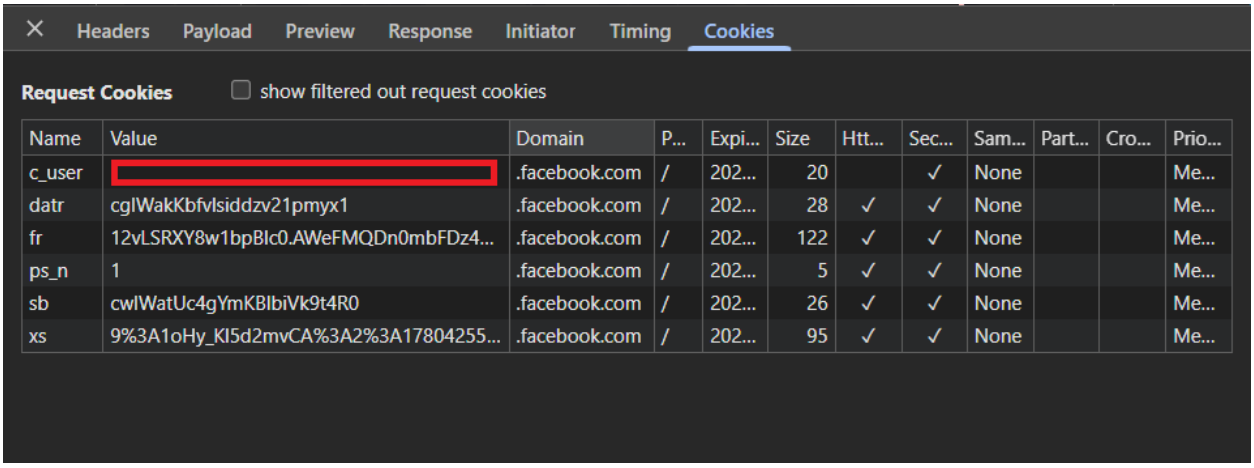


Figure 20 – Cookies transmitted the Facebook "PageView" event

98. When a business applies to use the Meta Pixel, it is provided with details about its functionality and its impact on private information.[56] Plaintiff and Website users, however, are not provided this information and would have no reason to look for it, as they are not a party to Defendant's agreement with Facebook.

99. To make use of the Meta Pixel, Defendant agreed to Facebook's Business Tool Terms (the "Facebook Terms").

100. The Facebook Terms inform website owners using the Meta Pixel that the employment of the Meta Pixel will result in data sharing, including with Facebook, through the automatic sharing of Pixel Event information and contact information.[57]

101. The Facebook Terms are transparent that Meta will use the Pixel Event information and contact information "to match the contact information against user IDs, as well as to combine those user IDs with corresponding [Pixel Event information]."[58]

102. Facebook directs parties implementing the Meta Pixel—here, Defendant—to encrypt request information[59] *before* data can be shared.[60]

103. Facebook further provides Meta Pixel users, such as Defendant, guidance on responsible data handling and details how data is acquired, used, and stored, including which information is shared with Facebook.

---

[56] *See Get Started*, META (last visited Feb. 17, 2026). (The Pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can their actions in the Facebook Ads Manager so you can use the data . . . . By default, the Pixel will track URLs visited [and] domains visited . . . .").

[57] *Meta Business Tools Terms*, FACEBOOK (Nov. 3, 2025) https://www.facebook.com/legal/terms/businesstools?paipv=0&eav=AfakosFmNyhZJOrkCsGodnMzth_uq6s403DsPEkeiKEyrj7rKyf5_t2I8wFEEUZUJlI&_rdr (last visited Feb. 17, 2026).

[58] *Id.*

[59] This contrasts with Facebook's JavaScript Pixel, which automatically encrypts the data being sent. Defendant has specifically chosen the Facebook Pixel method, which makes users' information visible. *See id.*

[60] *Id.*

104. Facebook educates or reminds Meta Pixel users of their responsibility to inform their users of their website's data sharing and specifically guides website owners to obtain the requisite rights, permissions, or consents before sharing information with any third party.[61]

105. As a sophisticated party entering into a business arrangement with another sophisticated party, Defendant was on notice of the potential privacy violations that would result from use of the Meta Pixel and ignored Facebook's warnings to safely handle its users' data and to warn its users that the Website would disclose information in a manner that threatened users' private information.

C. Google Tracking Tools

106. Google offers a range of advertising products, each serving a distinct function within advertising portfolios.

1. Google Ads

107. Google Ads, formerly AdWords, is an advertising platform developed by Google that allows advertisers to bid to display advertisements, service offerings, product listings, or videos to web users.[62]

108. The process advertisers using Google Ads to display ads within text-based search results is as follows: (i) advertisers create text-based ads with a title, description, and a link to the website to place within the Google search results; (ii) advertisers then choose keywords, usually related to their business or target audience, intended to trigger their ads to appear within the user's search results;[63] (iii) Google then allows advertisers to bid on those various keywords;[64] (iv) the

---

[61] *Best practices for privacy and data use for Meta Business Tools*, META, https://www.facebook.com/business/help/363303621411154?id=818859032317965 (last visited Feb. 17, 2026).
[62] *Achieve all your goals in one place*, GOOGLE, https://ads.google.com/home/goals/ (last visited May 6, 2026).
[63] *Be just a Google Search away*, GOOGLE, https://ads.google.com/home/campaigns/search-ads/ (last visited May 6, 2026).
[64] *Id*.

advertiser with the highest bid wins the auction, and the ad is displayed on the search results page; and (v) the winning ad appears above or below the organic search results and is marked as an ad.

109. Google AdSense works in conjunction with the Google Ads bidding system and allows website owners to display Google Ads on their websites and earn a revenue share when ads are viewed or clicked.[65] The search terms bid on through Google Ads are used by website owners participating in Google AdSense, allowing those owners to share in advertising revenue generated by Google.

110. AdSense for content or AdSense for search are methods by which AdSense functions.[66] In either configuration, AdSense matches advertisements to website users based on website content and user activity.

111. Google Ads intercepted Plaintiff's page views, as depicted below, using the sample webpage.

[65] *Google AdSense Home*, GOOGLE, https://www.google.com/adsense/start/how-it-works/ (last visited May 6, 2026).
[66] *AdSense revenue share*, GOOGLE, https://support.google.com/adsense/answer/180195?hl=en (last visited May 6, 2026).

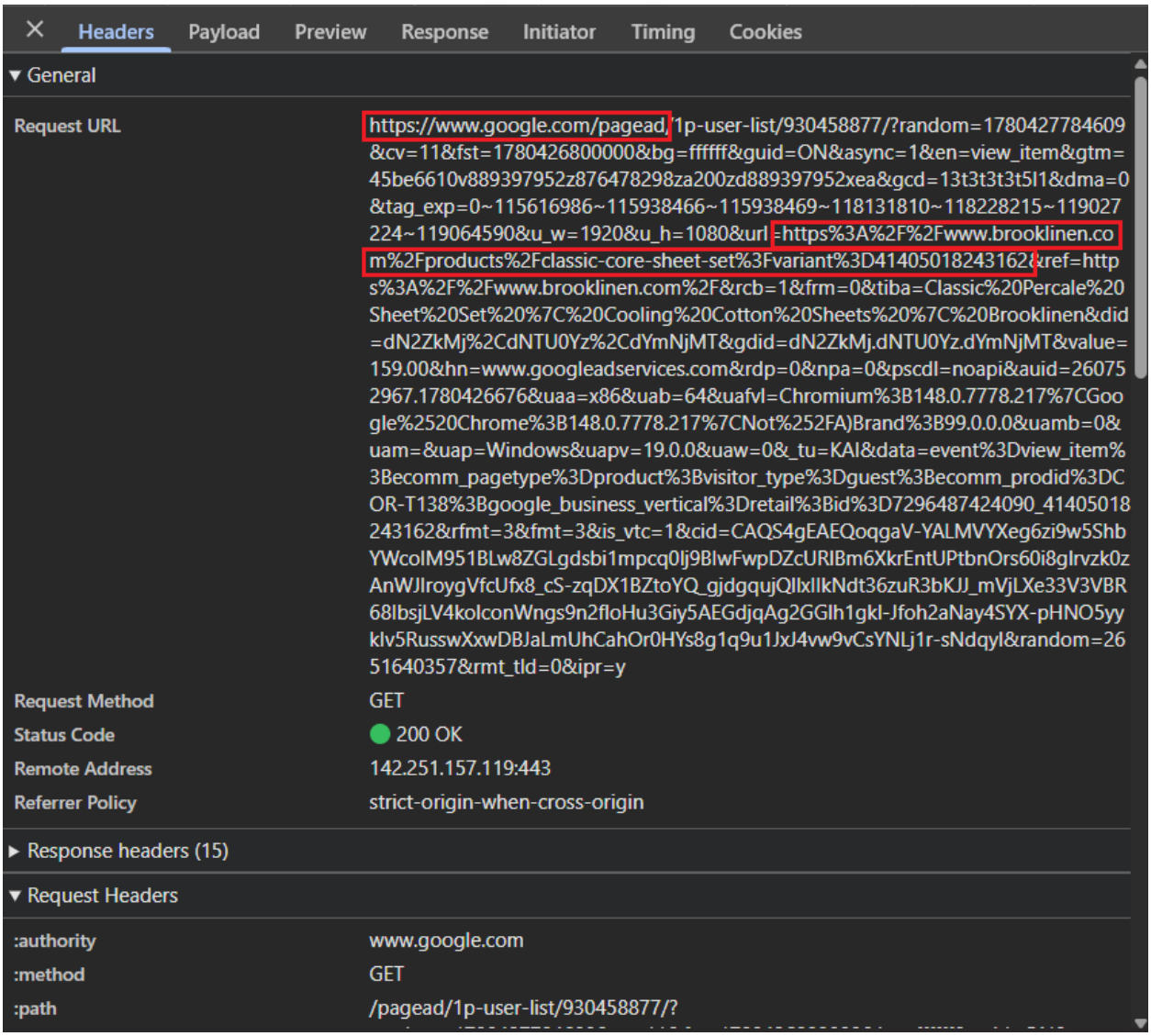


Figure 21 – Google Page Ads Intercepting communications on the Website

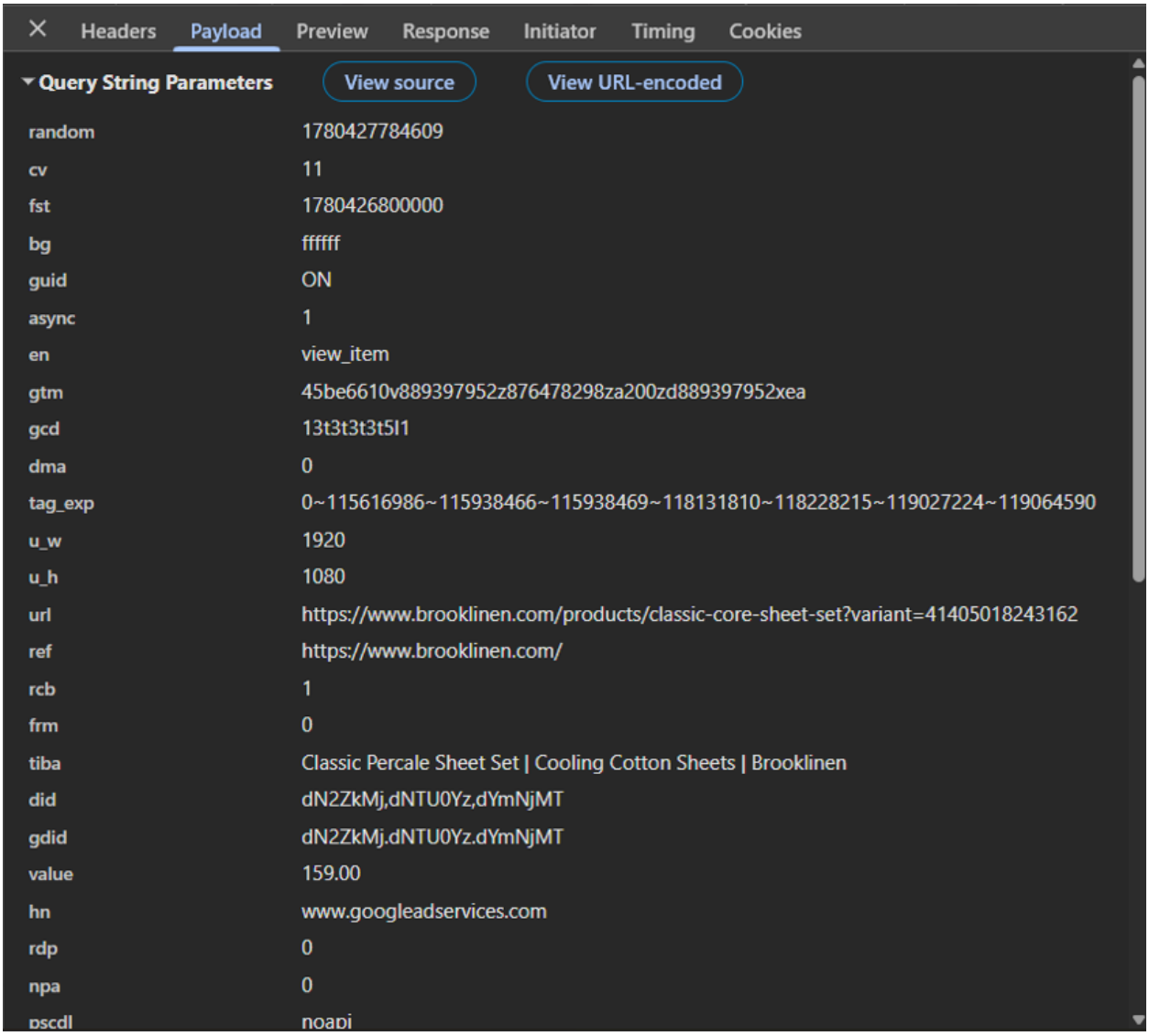


Figure 22– Content of Google Page Ad tracking a user landing on the product page of the Website

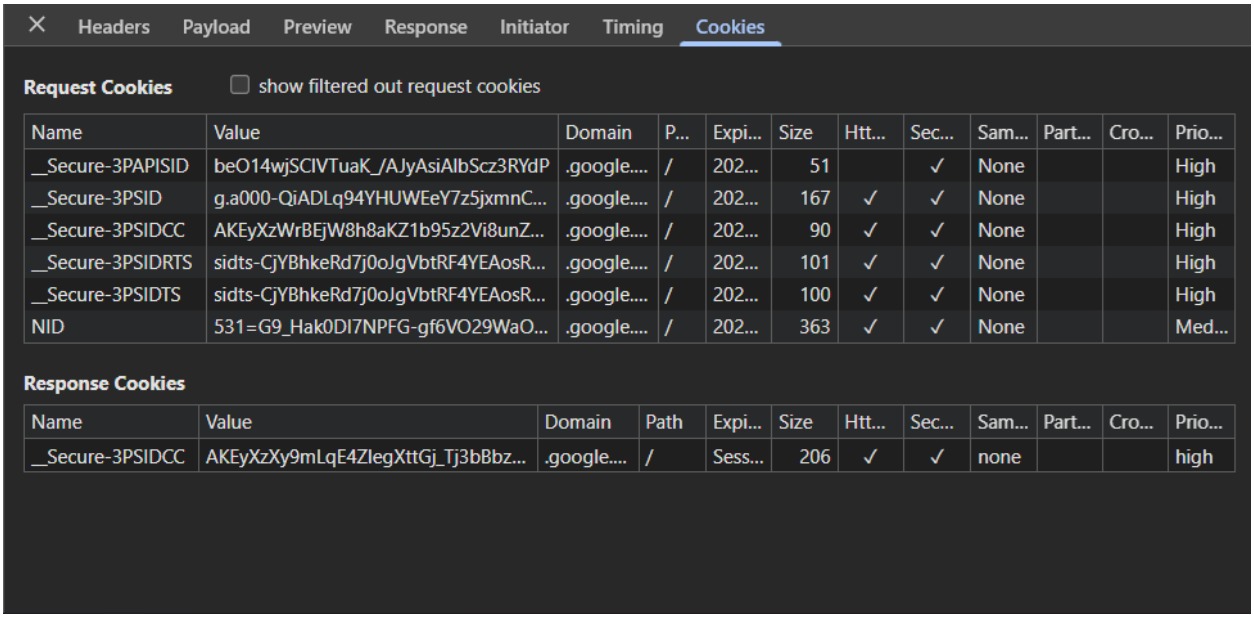


Figure 23 – Cookies transmitted by Google Page Ad on the Website

112. Google benefits when website owners utilize Google Ads and Google AdSense in connection with their websites.

113. Through Google AdSense, Google aggregates search data collected from website users. Google uses that data to improve its services and deliver more relevant search results. By analyzing patterns and trends in visitor behavior, Google gains insight into what users search for and what interests them. That insight supports service improvements, product development, and revenue growth.

114. Google's collection and analysis of search results also allows it to improve its machine learning algorithms.[67] Google uses data on how users interact with search results to train its algorithms to provide more accurate and relevant search results.[68] For example, when a user clicks on a particular search result and spends more time on that page, Google treats that interaction as a signal of relevance to the search query. By aggregating such data across users,

[67] Elle Poole Sidell, *What Does Google Do With Your Data?*, AVAST (Dec. 18, 2020) https://www.avast.com/c-how-google-uses-your-data (last visited May 6, 2026).
[68] *Id.*

Google can develop advertising profiles that include demographic and interest-based attributes, such as age range, industry, and interests.[69]

115. Google profits in several ways from the Website's use of the Google search engine: (i) advertisers bid and pay Google for the keywords that will result in their ads showing in search results; (ii) through AdSense search, every time a user clicks or views an ad (depending on their chosen method), the advertiser will pay Google for that click or view; (iii) and Google's ability to aggregate user search data allows Google to further tailor its products to advertisers and users by training its algorithms on large volumes of search data.

2. Google Analytics

116. Google Analytics ("GA") collects data about visitor interactions with a website. That data includes link clicks, button clicks, form submissions, conversions, shopping cart abandonment, items added to or removed from carts, file downloads, scrolling behavior, video views, call-to-action performance, table-of-contents clicks, and other customizable events.[70]

117. GA transmits collected interaction data to Google, which associates the activity with the website that generated it.[71] Notably, Google notifies web developers that developers should provide "users with clear and comprehensive information about the data . . . collect[ed] on [their] websites" and to obtain "consent for that collection where legally required."[72]

118. GA functions through specific collection settings and fixed data transmission paths. Google acknowledges the legal implications of those practices and assigns responsibility for visitor disclosure to website developers, including Defendant.

---

[69] *Id*.
[70] Zach Paruch, *What Is Google Tag Manager & How Does It Work?*, SEMRUSH BLOG (Jan. 4, 2024) https://www.semrush.com/blog/beginners-guide-to-google-tag-manager/ (last visited May 6, 2026).
[71] *About the Google tag*, GOOGLE, https://support.google.com/tagmanager/answer/11994839?hl=en (last visited May 6, 2026).
[72] *Id.*

119. Here, Defendant added GA to the Website. That implementation caused Plaintiff's webpage views to be intercepted and transmitted to Google, as shown by the example taken directly from the Website below:

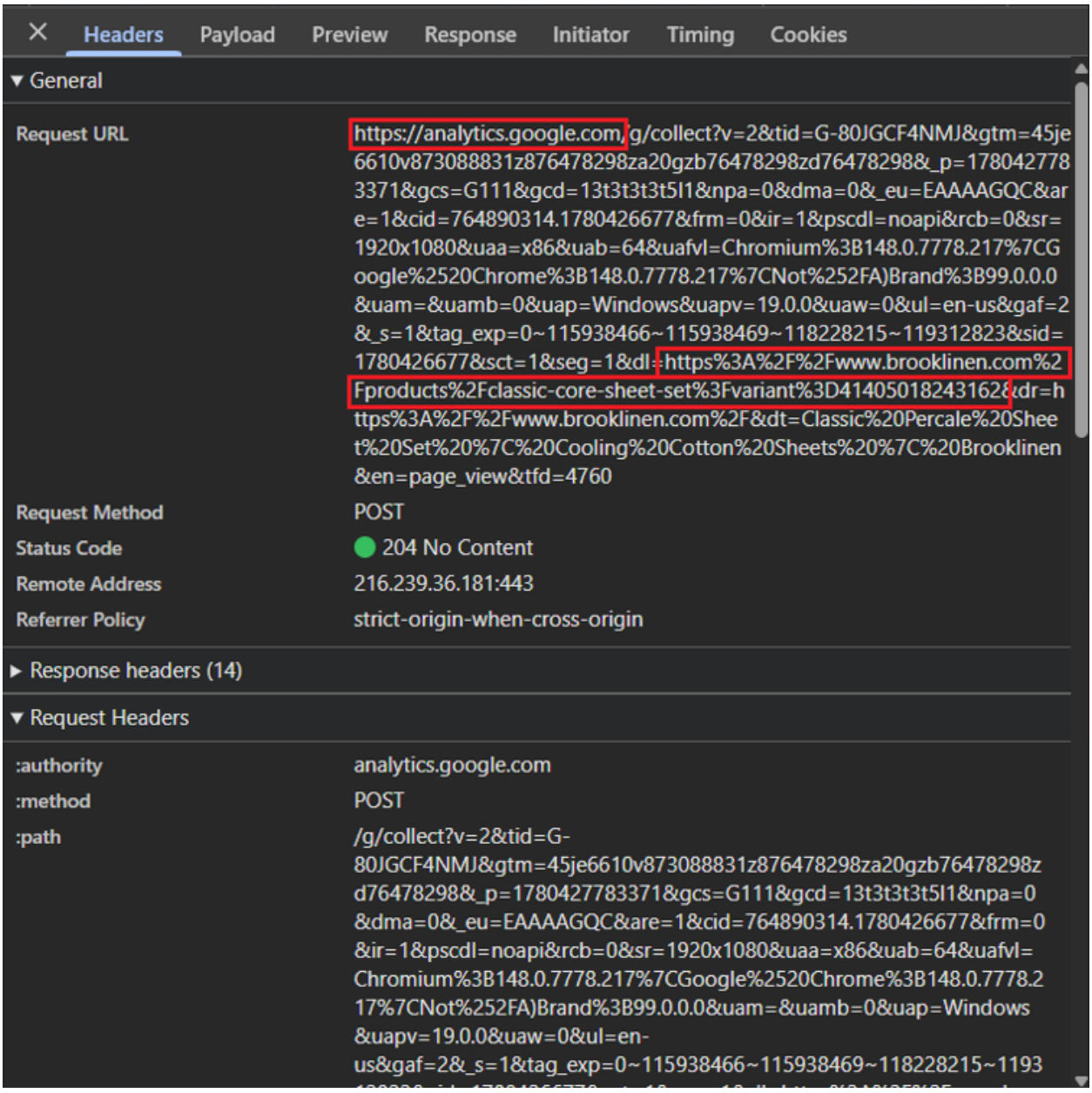


Figure 24 – Google Analytics capturing communications on the Website

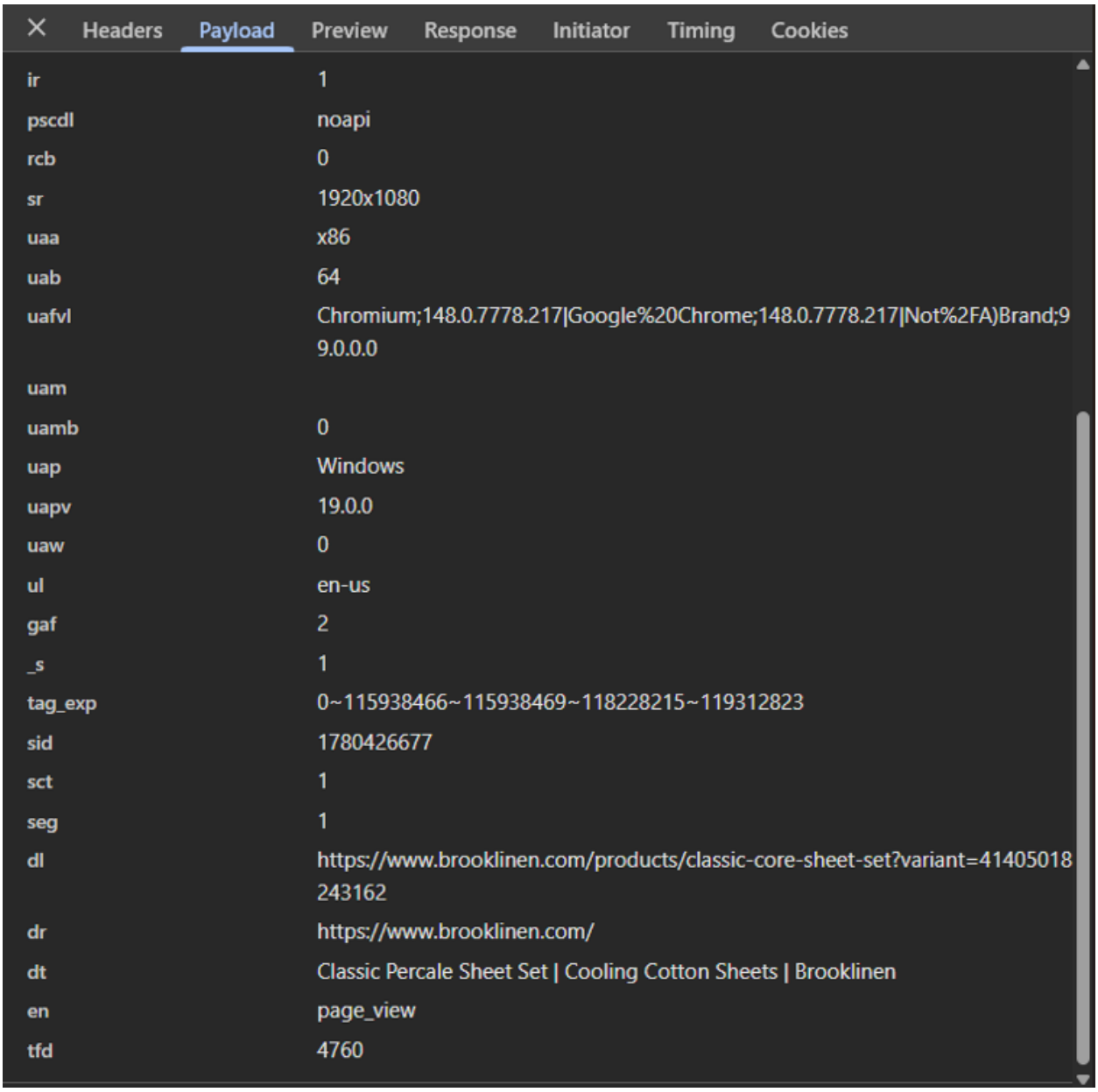
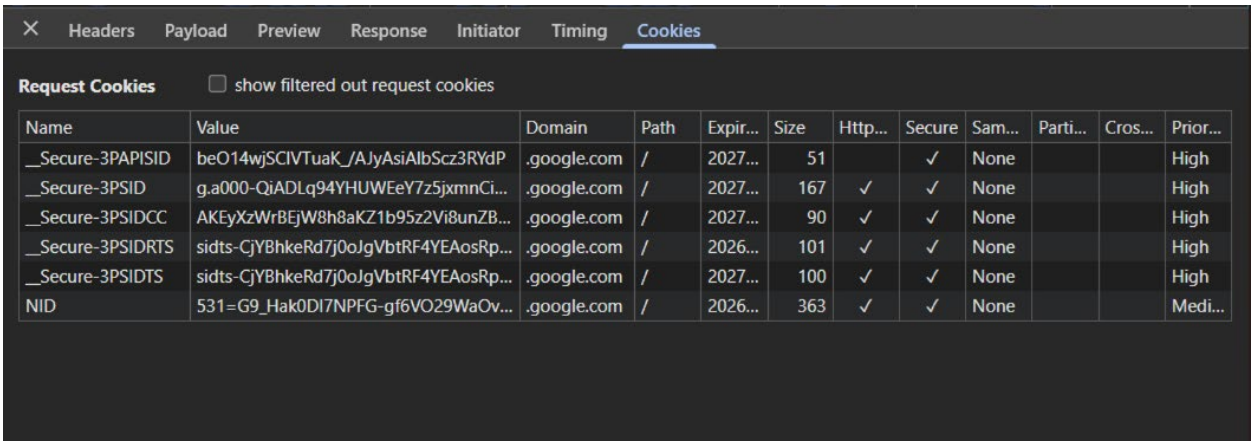


Figure 25 – Information captured when Google Analytics captures communications on the Website



Name	Value	Domain	Path	Expir...	Size	Http...	Secure	Sam...	Parti...	Cros...	Prior...
__Secure-3PAPISID	beO14wjSCIVTuaK_/AJyAsiAIbScz3RYdP	.google.com	/	2027...	51		✓	None			High
__Secure-3PSID	g.a000-QiADLq94YHUWEeY7z5jxmnCi...	.google.com	/	2027...	167	✓	✓	None			High
__Secure-3PSIDCC	AKEyXzWrBEjW8h8aKZ1b95z2Vi8unZB...	.google.com	/	2027...	90	✓	✓	None			High
__Secure-3PSIDRTS	sidts-CjYBhkeRd7j0oJgVbtRF4YEAosRp...	.google.com	/	2026...	101	✓	✓	None			High
__Secure-3PSIDTS	sidts-CjYBhkeRd7j0oJgVbtRF4YEAosRp...	.google.com	/	2027...	100	✓	✓	None			High
NID	531=G9_Hak0DI7NPFG-gf6VO29WaOv...	.google.com	/	2026...	363	✓	✓	None			Medi...

Figure 26 – Cookies transmitted by Google Analytics on the Website.

120. After the data reaches those common destinations, Google products analyze the information and provide feedback that allows Defendant to monetize the collected data through targeted advertising.

D. Microsoft UET

121. Microsoft offers Microsoft Advertising (formerly known as "Bing Advertising"), a platform where advertisers can display ads to consumers across the internet based on their search terms and interests.[73]

122. One of the software tools available through Microsoft Advertising is Universal Event Tracking ("UET"), which allows website owners, like Defendant, to allow Microsoft to track conversion events on a website, target specific audiences, and automate advertisement bidding.[74]

123. UET is a tag that is placed on a website. Once UET is installed, the tag reports all users' activity on the website to Microsoft Advertising.[75]

---

[73] *Bing Ads API Overview,* MICROSOFT, https://learn.microsoft.com/en-us/advertising/guides/?view=bingads-13 (last visited Feb. 25, 2026).
[74] *What is UET and how can it help me?,* MICROSOFT, https://help.ads.microsoft.com/#apex/ads/en/56681/2 (last visited Feb. 25, 2026).
[75] *What is UET and how does it related to conversion tracking and remarketing features?,* MICROSOFT, https://help.ads.microsoft.com/#apex/ads/en/53056/2-500 (last visited Feb. 25, 2026).

124. UET uses several cookies, which it stores and/or accesses on website visitors' browsers. These cookies include the MR cookie, the MUID cookie, which contains a global unique ID assigned to a visitor's browser that identifies them,[76] the _uetsid cookie, which contains a session ID, and the _uetvid, which contains a unique ID for a unique website visitor.[77]

125. UET can collect a vast amount of data from website visitors. The MUID/GUID cookie and the visitor's IP address are always passed to Microsoft with every HTTP request from UET. UET can also collect:

- Event actions
- Event categories
- Event types
- Browser language setting
- Page URLs
- Referrer URLs
- Screen height
- Session ID
- The UET tag ID
- A signed-in user's ID
- A visitor ID[78]

126. Defendant's use of UET on the Website is shown in the figures below.

---

[76] *Guid Struct,* MICROSOFT, https://learn.microsoft.com/en-us/dotnet/api/system.guid?view=net-10.0 (last visited Mar. 3, 2026).
[77] *What cookies does UET use?,* MICROSOFT, https://help.ads.microsoft.com/#apex/ads/en/53056/2-500 (last visited Feb. 25, 2026).
[78] *What data does UET collect once I install it on my Website?,* MICROSOFT, https://help.ads.microsoft.com/#apex/ads/en/53056/2-500 (last visited Feb. 25, 2026).

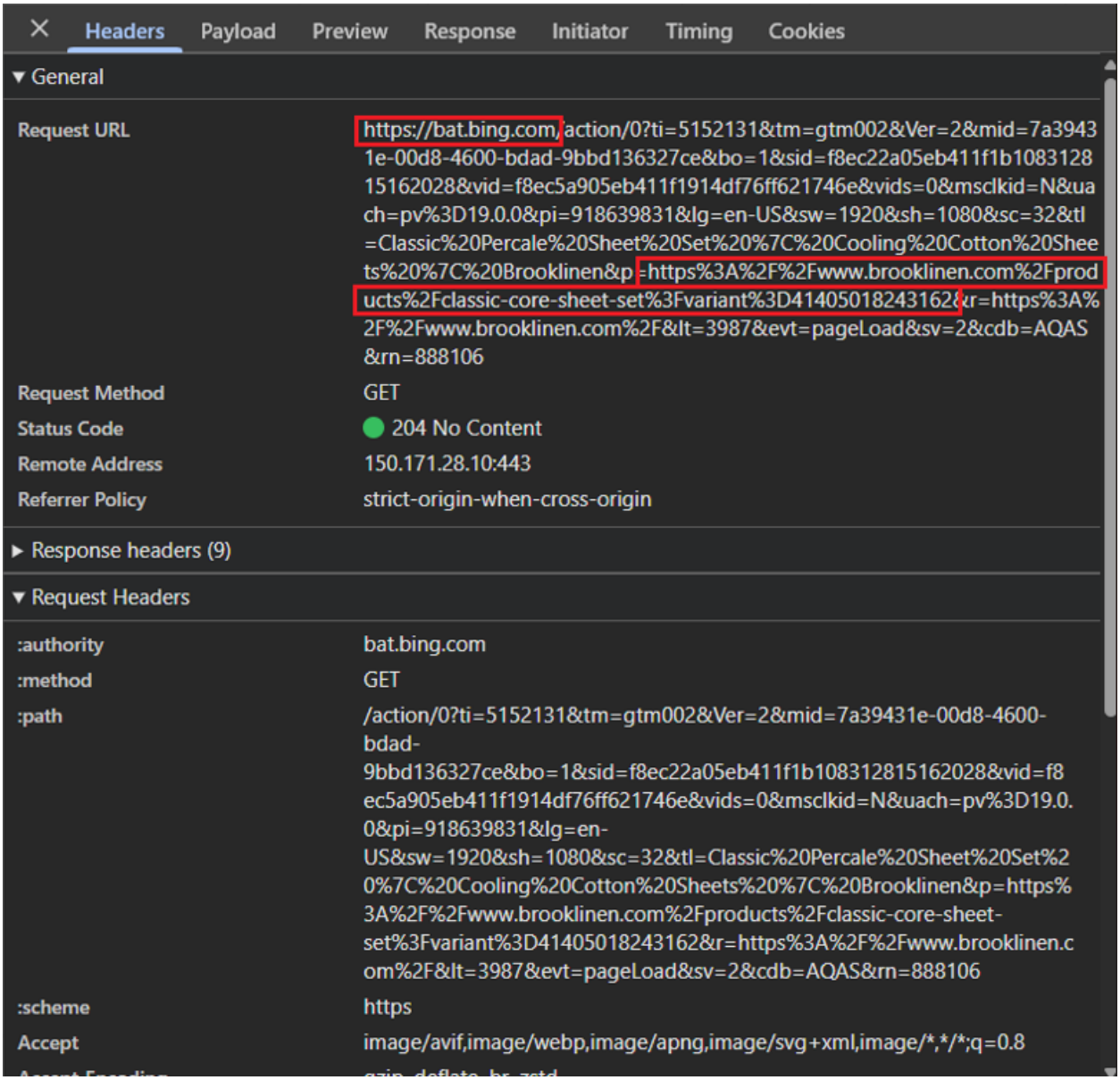


Figure 27 – UET tracking users' communications on the Website

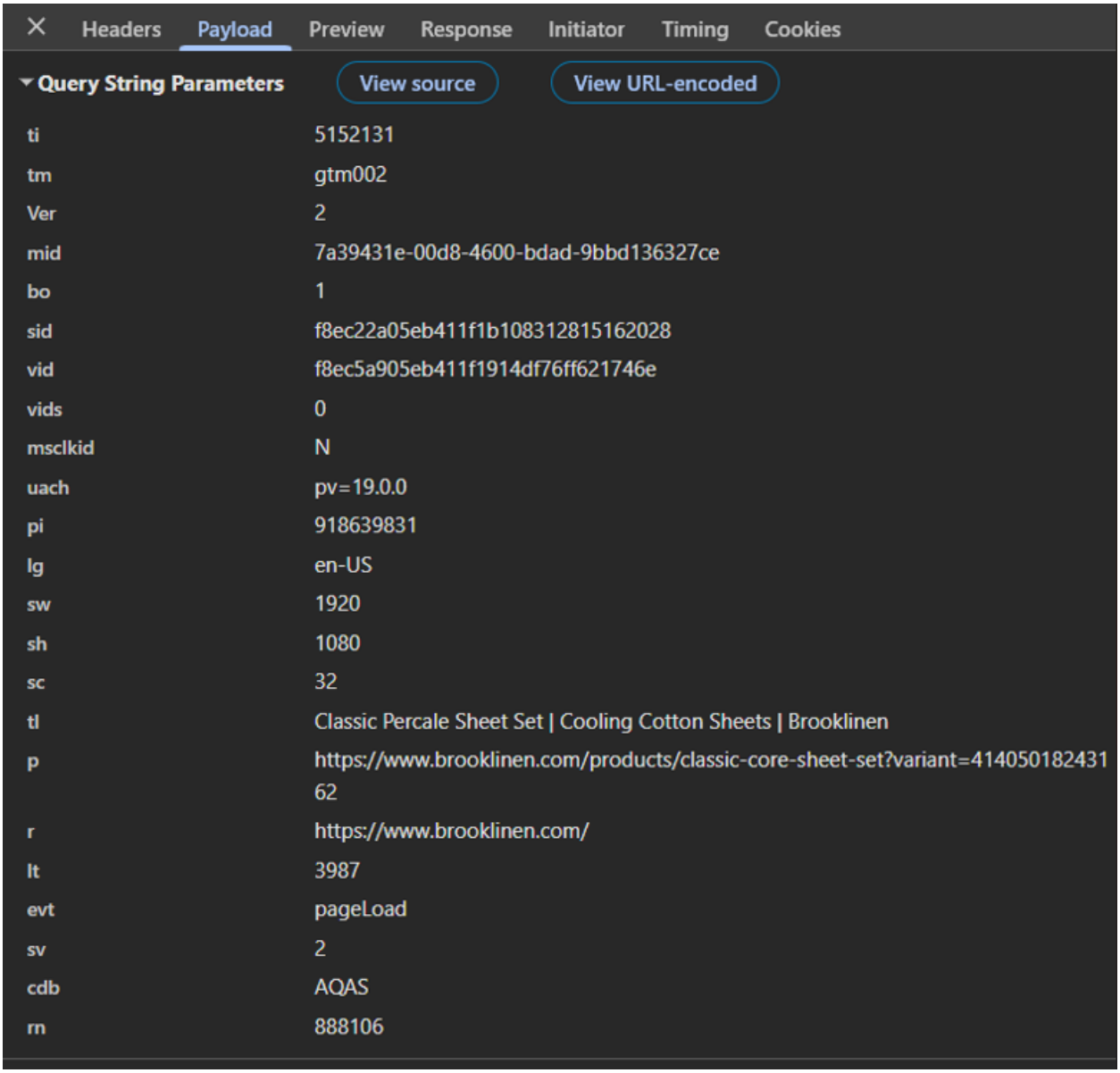


Figure 28 – Information intercepted by UET tracking users' communications on the Website

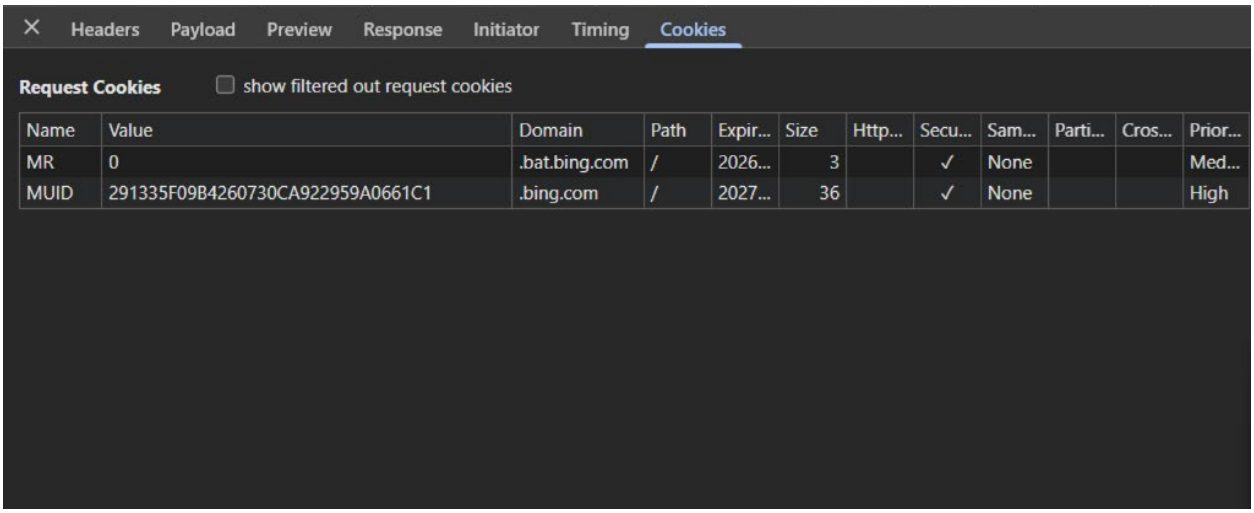


Figure 29 – Cookies transmitted by UET on the Website

127. Microsoft informs UET-using websites that they are responsible for managing visitor consent. Websites are instructed to place the "_uetmsdns" cookie as a first-party cookie and set the value to 1 to stop events from firing and respect visitor consent choices, should they not accept the use of trackers.[79]

128. Defendant failed to place this cookie on the Website and did not stop UET events from firing when visitors declined the use of cookies.

1. The Pinterest Tag

129. Defendant installed a tracking pixel on its Website created by the social media site, Pinterest (the "Pinterest Tag").

130. The Pinterest Tag is a piece of code a website owner can add to their site to track visitors and record their actions, so they can later target them with ads on Pinterest.[80]

[79] *How can I stop UET events from being fired for users who request to restrict data sharing?,* MICROSOFT, https://help.ads.microsoft.com/#apex/ads/en/53056/2-500 (last visited Feb. 25, 2026).
[80] *Install the Pinterest tag*, PINTEREST, https://help.pinterest.com/en/business/article/install-the-pinterest-tag (last visited Dec. 22, 2025).

131. To use the Pinterest Tag, a website owner must include the Pinterest Tag ID in the base code of their website.[81]

132. The Pinterest tag ID identifies which code needs to be sent to the user's browser to track website owner-designated data points through specified "events,"[82] and to establish which Pinterest account will receive the data upon collection.[83]

133. Once a website owner adds the base code of the Pinterest Tag, they can add "event codes" so the Pinterest Tag tracks specific actions visitors take on their website, such as viewing a page, watching a video, checking out, and other specified events.[84]

134. The Pinterest Tag begins intercepting user information as soon as it loads in users' browsers.[85]

135. Website owners, like Defendant, then send the collected information to Pinterest. Pinterest recommends that website owners transmit the IP address of website visitors for all conversion events.[86]

136. Without implementing any other features, the Pinterest Tag tracks and transmits the URL currently being viewed by the website visitor. Additionally, the Pinterest Tag reads and

[81] *Add the base code to your website*, PINTEREST, https://help.pinterest.com/en/business/article/install-the-base-code (last visited Dec. 22, 2025).
[82] *Add event* codes, PINTEREST, https://help.pinterest.com/en/business/article/add-event-codes (last visited Dec. 22, 2025)
[83] *See Add the base code to your website*, PINTEREST, https://help.pinterest.com/en/business/article/install-the-base-code (last visited Dec. 22, 2025); *Set up the Pinterest tag with Google Tag Manager*, , https://help.pinterest.com/en/business/article/google-tag-manager-and-pinterest-tag (highlighting that integrating Pinterest Tags with third party data tracking systems requires a Pinterest tag ID to know which Pinterest conversion account should receive the tracked data) (last visited Dec. 22, 2025).
[84] *Add event* codes, PINTEREST, https://help.pinterest.com/en/business/article/add-event-codes (last visited Dec. 22, 2025).
[85] *Pinterest tag*, PINTEREST, https://developers.pinterest.com/docs/api-features/pinterest-tag/#:~:text=The%20Pinterest%20Tag%20allows%20you,Pinterest%20Tag%20has%20two%20components: (last visited Dec, 22, 2025).
[86] *Track conversion events*, PINTEREST, https://developers.pinterest.com/docs/api-features/track-conversion-events/ (last visited Dec. 22, 2025).

uses first-party cookies to identify the Pinterest user currently viewing the website through a personalized Pinterest "User ID," even when the user is logged out of Pinterest.[87]

137. Website owners can also, in conjunction with the Pinterest Tag, enable a feature called "automatic enhanced match" to identify the exact identities of Pinterest users who visit the website.[88]

138. When used in conjunction with automatic enhanced match, the Pinterest Tag collects and transmits to Pinterest the following user data:

a. Email addresses;

b. First and last names;

c. Phone numbers;

d. Genders;

e. Birth dates;

f. External IDs; and address location information such as city, state, zip code, and country.[89]

139. This data can be used by Pinterest to "match more of [a] website['s] visitors and conversions to people on Pinterest, which can lead to improvements in [ad] campaign performance . . . and audience reach . . . ." [90]

140. Pinterest uses this data to help advertisers like Defendant gauge the effectiveness of their ad campaigns, optimize the return on their ad spending, and broaden their audience reach.[91]

---

[87] *View tag parameters and cookies*, PINTEREST, https://help.pinterest.com/en/business/article/pinterest-tag-parameters-and-cookies (last visited Dec.22, 2025).
[88] *Enable automatic enhanced match*, PINTEREST, https://help.pinterest.com/en/business/article/automatic-enhanced-match (last visited Dec. 22, 2025).
[89] *Id.*
[90] *Id.*
[91] *Id.*

141. The Pinterest Tag also sends the "tid" parameter, which identifies the website owner's Pinterest Tag ID.[92] Here, the "tid" parameter, found in Pinterest Tag transmissions from Defendant's site, contains Defendant's Pinterest tag ID of 2612948917583. This data is sent both when the Website receives communications and when users send communications to the Website.

142. Additionally, unless websites use a specific "limited data processing flag," Pinterest uses this data, such as names, phone numbers, emails, and IP addresses, to conduct research on Pinterest usage and to market its own services.[93]

143. Pinterest also sends the data to its business partners and other vendors.[94] Defendant's use of the Pinterest Tag on the Website is demonstrated below:

[92] Pinterest tag parameters and cookies, , https://help.pinterest.com/en/business/article/pinterest-tag-parameters-and-cookies (last visited Dec. 12, 2025). *Pinterest tag parameters and cookies*, PINTEREST, https://help.pinterest.com/en/business/article/pinterest-tag-parameters-and-cookies (last visited Dec. 22, 2025).
[93] *Limited data processing*, PINTEREST, https://help.pinterest.com/en/business/article/limited-data-processing (last visited May 17, 2025).
[94] *California Privacy Statement and Notice at Collection*, PINTEREST, https://policy.pinterest.com/en/notice-at-collection (last visited Dec. 22, 2025).

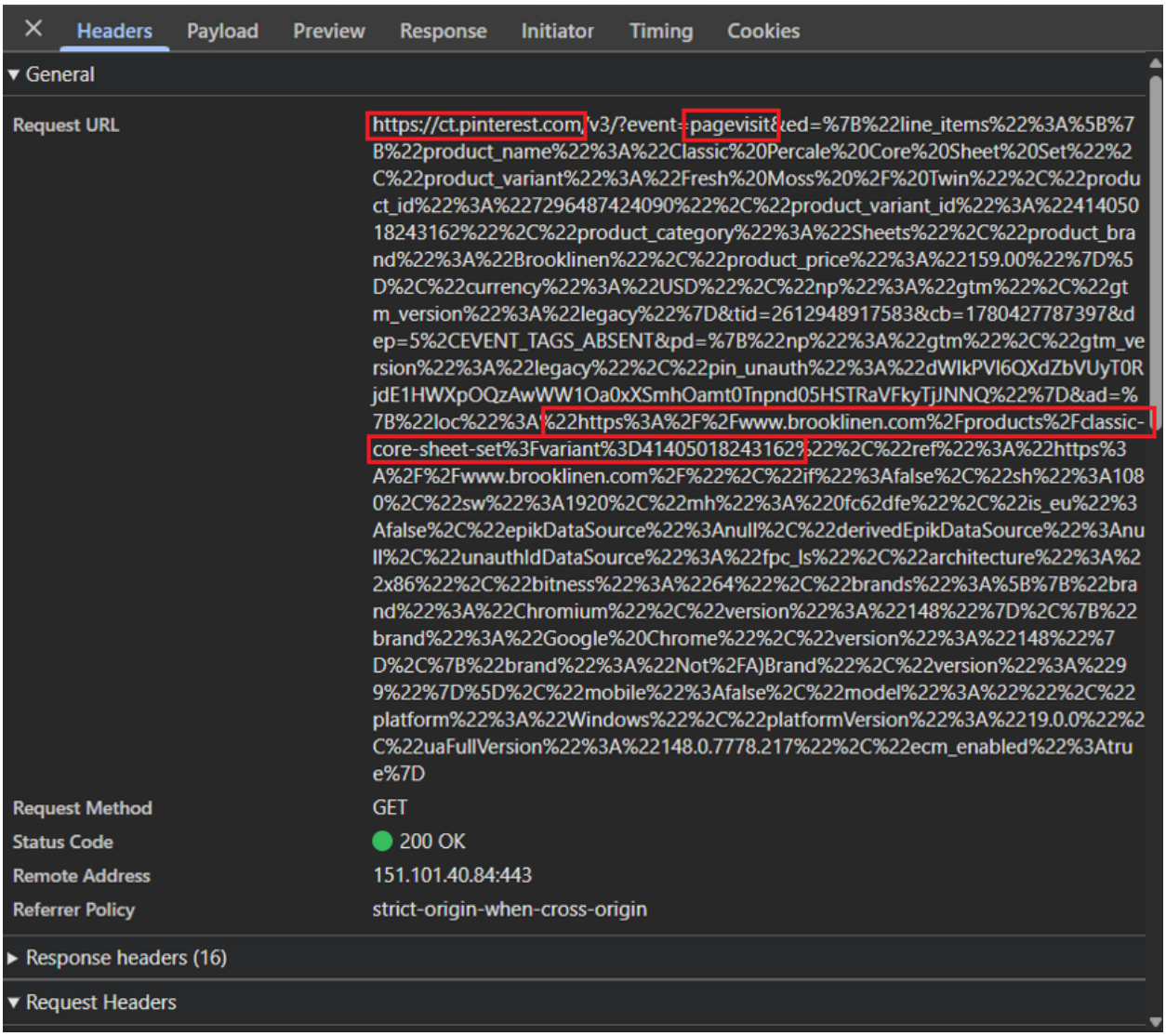


Figure 30 – Pinterest Tag tracking a user landing on the Website

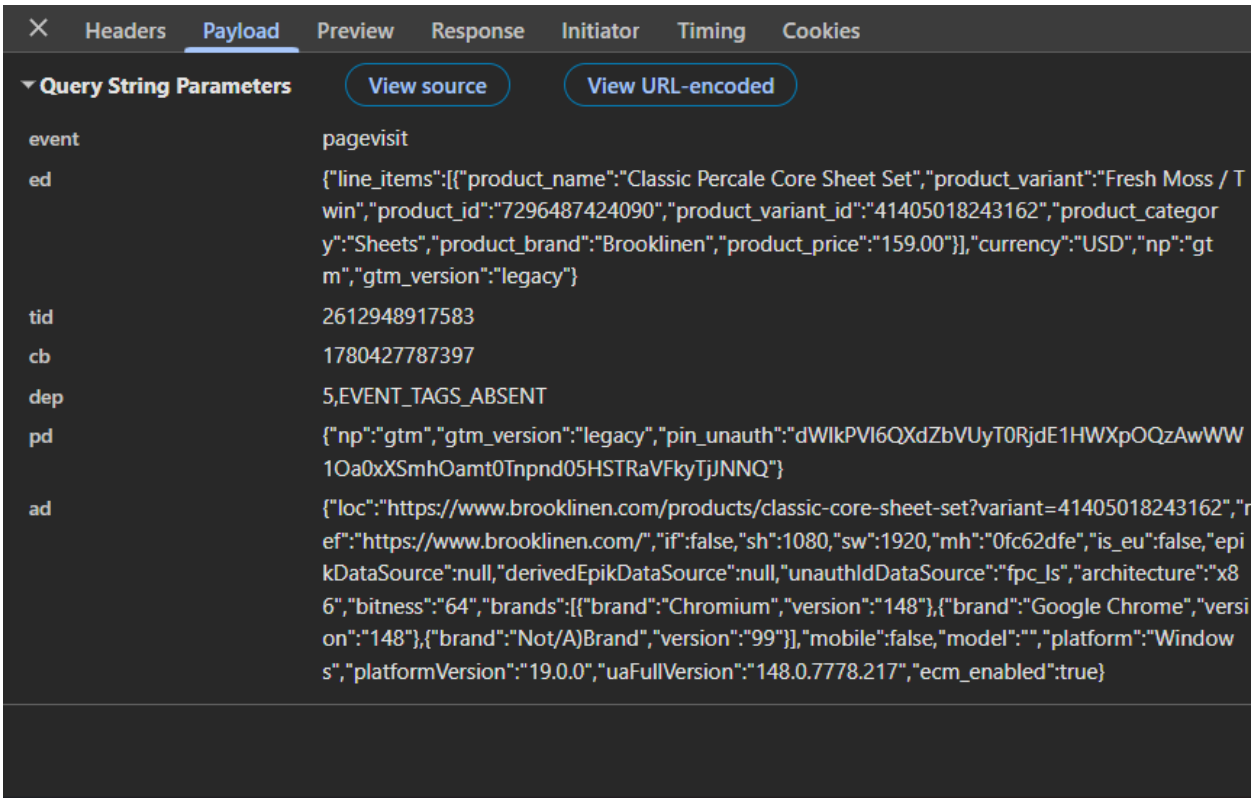


Figure 31– Information intercepted by the Pinterest Tag tracking a user landing on the webpage

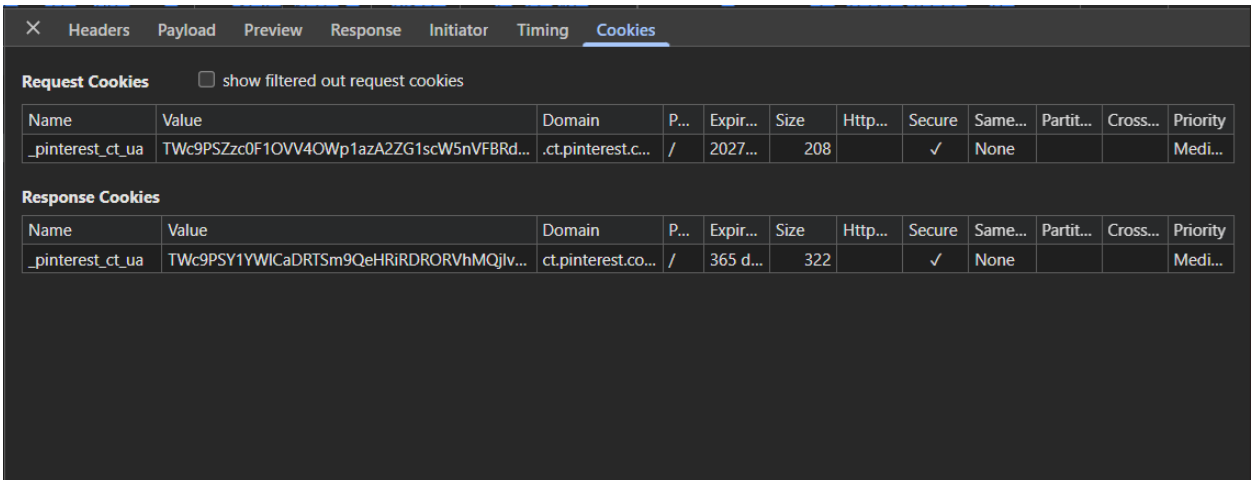


Figure 32 – Cookies transmitted by the Pinterest Tag on the Website

144. When a website owner applies to Pinterest to use the Pinterest Tag, the website owner must agree to Pinterest's Developer and API Terms of Service (the "Pinterest Terms"), part of which requires agreeing that Pinterest may collect and use website users' information.[95]

145. The Pinterest Terms further provide Pinterest Tag users, like Defendant, with guidance on their privacy responsibilities.

146. Pinterest directs parties implementing the Pinterest Tag, such as Defendant, to clearly disclose their data practices and obtain their users' consent where required by law.[96]

147. As a sophisticated party entering into a business arrangement with another sophisticated party, Defendant was on notice of the potential privacy violations that would result from use of the Pinterest Tag, and ignored Pinterest's warnings to safely handle its users' data and to warn its users that the Website would disclose information in a manner that threatened users' private Sensitive Information.

E. The Reddit Pixel

148. Additionally, Defendant has installed a tracking pixel on its Website created by social media platform Reddit (the "Reddit Pixel").

149. The Reddit Pixel is a piece of code that a website owner can add to their site to allow Reddit to track users on the site and record the actions visitors take in their browsers.[97] The harvested data is subsequently used by Reddit and the website owner to serve targeted ads to Reddit users.

---

[95] *Developer and API Terms of Service*, PINTEREST, https://developers.pinterest.com/terms/ (last visited Dec. 22, 2025).
[96] *Id.*
[97] *About the Reddit Pixel*, REDDIT, https://business.reddithelp.com/s/article/reddit-pixel (last visited Feb. 17, 2026); *Install the Reddit Pixel Directly*, REDDIT, https://business.reddithelp.com/s/article/Install-the-Reddit-Pixel-on-your-website (last visited Feb. 17, 2026).

150. The Reddit Pixel is also used in conjunction with Reddit's Conversion API (CAPI) to track specific actions that users take on the websites, such as viewing a page, submitting a search in the website's search bar, adding a product to the visitor's cart, checking out, and other specified events.[98] Because the Reddit CAPI operates on website servers, users cannot verify its use.

151. Reddit makes use of a website owner's pixel ID to determine which data should be tracked when sending the code for the Pixel to the user's browser,[99] and to specify "which business account should receive" the user's tracking data.[100]

152. Reddit admits that it shares users' Sensitive Information with third and fourth parties,[101] just as Plaintiff's Sensitive Information was shared here.

153. In Defendant's use of the Reddit Pixel, Defendant configured the Reddit Pixel to include a parameter called "id" which identifies Defendant's Reddit Pixel ID as "t2_s7oxe". This data is sent both when the Website receives communications and when users send communications to the Website.

154. Website owners, like Defendant, can enable a feature of the Reddit Pixel called "Auto-Advanced Matching" to determine the exact identities of Reddit users who visit the website.

155. Auto-Advanced Matching automatically scrapes a website for any email addresses a user types or pastes and sends that email information to Reddit.[102]

---

[98] *Conversion Events*, REDDIT, https://business.reddithelp.com/articles/Knowledge/supported-conversion-events (last visited Feb. 17, 2026).
[99] *See Install the Reddit Pixel Directly*, REDDIT, https://business.reddithelp.com/s/article/Install-the-Reddit-Pixel-on-your-website (last visited Feb. 17, 2026).
[100] *About the Reddit Pixel*, REDDIT, https://business.reddithelp.com/s/article/reddit-pixel (last visited Feb. 17, 2026).
[101] Reddit Privacy Policy, REDDIT (Jan. 6, 2026), https://www.reddit.com/policies/privacy-policy (last visited Feb. 26, 2026).
[102] *Auto-Advanced Matching*, REDDIT, https://business.reddithelp.com/s/article/automated-advanced-matching (last visited Feb. 17, 2026).

156. In addition to email addresses, a website owner can enable the Reddit Pixel and the CAPI to send additional personal information to Reddit, known as "match keys," to identify website users.[103]

157. IP addresses are match keys that website owners are *required* to send to Reddit. Website owners and Reddit may also use other match keys, including:

a. Email addresses;

b. Phone numbers;

c. Mobile Advertising IDs (a unique identifier for a mobile user);

d. Reddit Click IDs (to attribute click conversions more accurately);

e. External IDs (an advertiser-assigned identifier that enhances match accuracy);

f. Reddit UUIDs (a unique ID generated by the Reddit Pixel);

g. User Agents (which identify the software the user is using to access the website); and

h. The visitor's screen dimensions.[104]

158. This data can be used by Reddit to match an otherwise anonymous website visitor to their Reddit account, or even to identify them outright, associating their identity with their activity on the website.

159. Reddit uses this data to help advertisers, including Defendant, gauge the effectiveness of their ad campaigns, improve their ability to attribute activity to specific campaigns, track users across devices, and create more precisely targeted campaigns.[105]

---

[103] *About Match Keys*, REDDIT, https://business.reddithelp.com/s/article/about-match-keys#customer-match-keys-and-identifiers (last visited Feb. 17, 2026).
[104] *Id.*
[105] *Id.*

160. Additionally, Reddit employs this data to optimize its own ad placements and to develop new services.[106]

161. Defendant's use of the Reddit Pixel on the Website is demonstrated by the screenshots below, which follow a user's journey to searching for and purchasing a product on the Website.

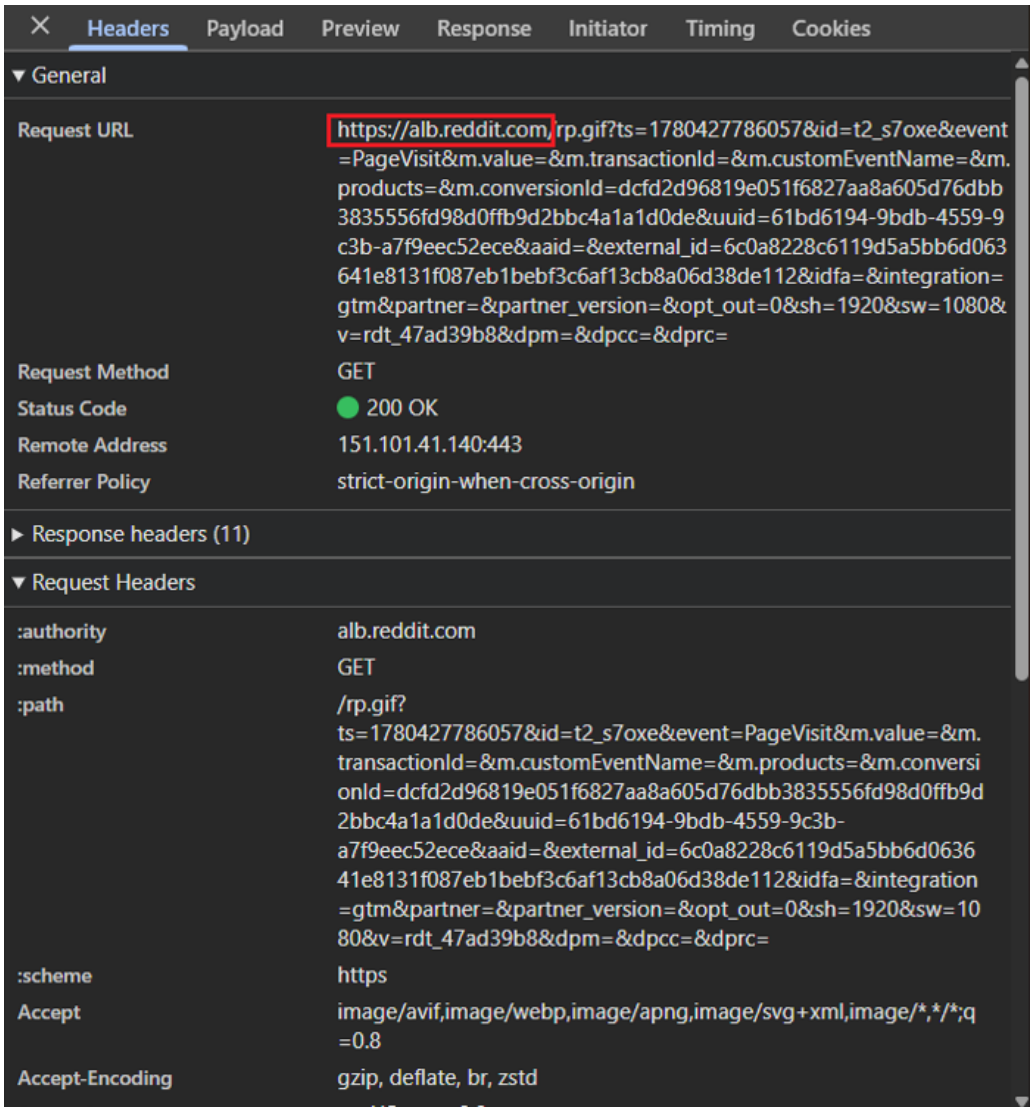


Figure 33 – Reddit Pixel tracking a user on the Website

[106] *Reddit Privacy Policy*, REDDIT (last revised Jan. 6, 2026) https://www.reddit.com/policies/privacy-policy#policy-h2-4 (last visited Feb. 17, 2026).

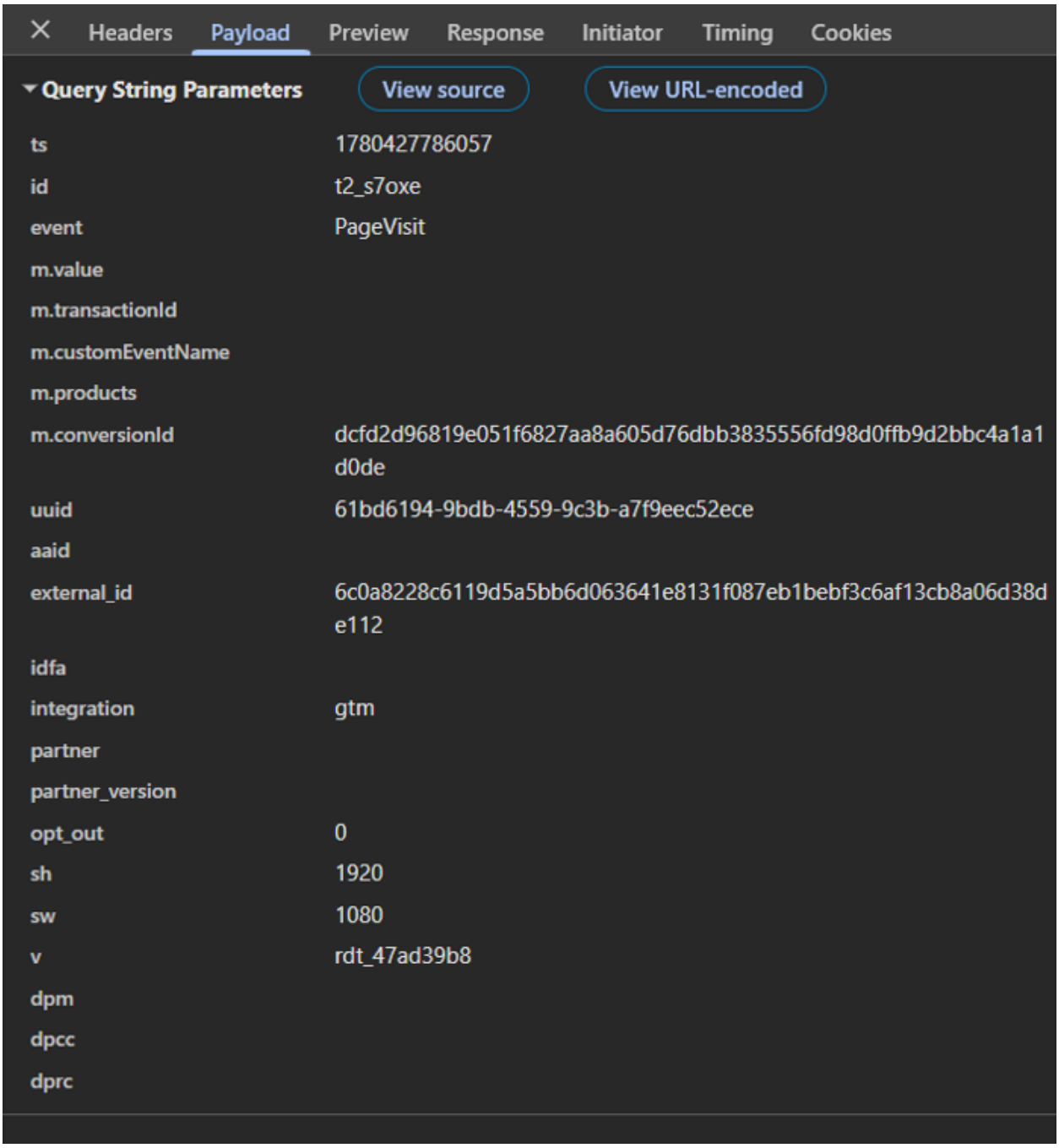


Figure 34 – Information intercepted by the Reddit Pixel tracking a user on the Website

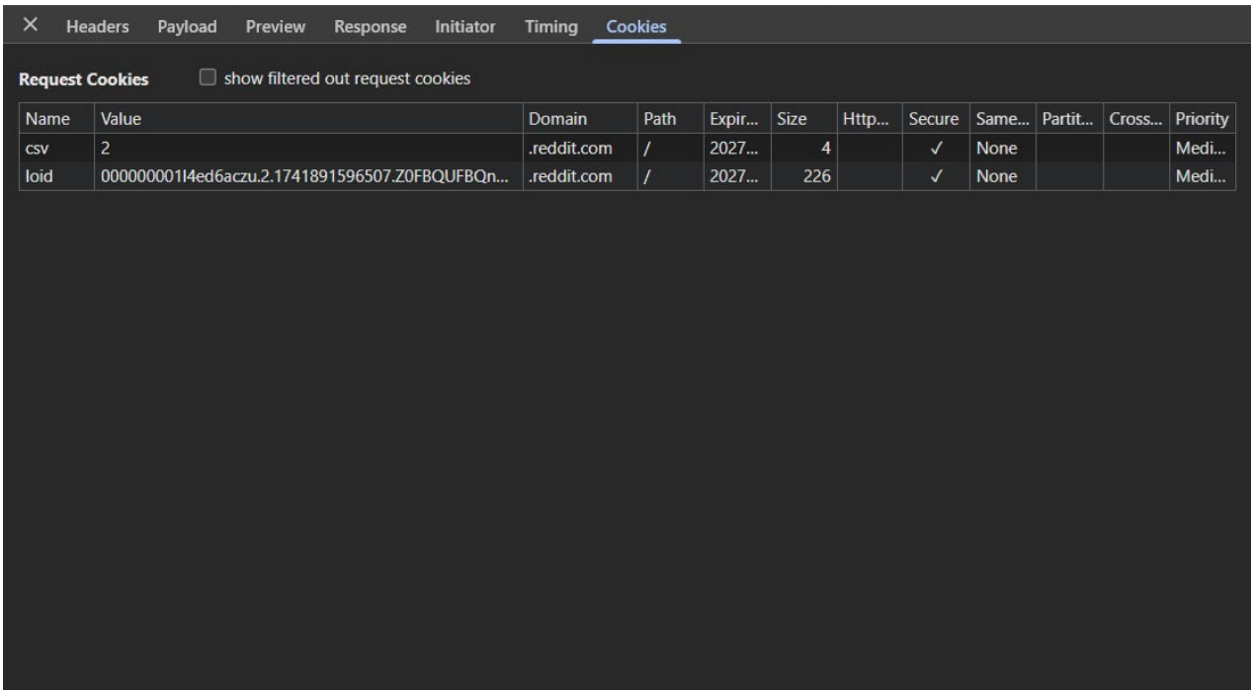


Figure 35 – Cookies transmitted by the Reddit Pixel on the Website

162. To utilize the Reddit Pixel, Defendant agreed to Reddit's Business Tool Terms (the "Reddit Terms").

163. The Reddit Terms inform website owners, such as Defendant, that the employment of the Reddit Pixel will result in Reddit obtaining users' data, including users' website actions, email addresses, cookie IDs, and device IDs, among other "matching parameters."[107]

164. The Reddit Terms make clear that the onus is on the Defendant to provide all necessary transparency notices and obtain all necessary rights, permissions, and lawful bases, including consent, to share information with Reddit.

165. The Reddit Terms explicitly condition the use of the Reddit Pixel on website owners' warranties that they: (i) provide "prominent and legally-sufficient notice" of the Reddit Pixel's data sharing to users; (ii) provide "clear, prominent and legally sufficient instructions

[107] *Reddit Business Tool Terms*, REDDIT (effective date Aug. 7, 2025; last revised July 7, 2025) https://business.reddithelp.com/s/article/Reddit-Business-Tool-Terms (last visited Feb. 17, 2026).

regarding how to opt out of data collection and use of such data collection and use;" and (iii) do not share "any data related to users who have not provided consent[.]"[108]

166. As a sophisticated party entering into a business arrangement with another sophisticated party, Defendant was on notice of the potential privacy violations that would result from use of the Reddit Pixel and ignored Reddit's warnings to safely handle its users' data and to warn its users that the Website would disclose information in a manner that threatened users' private information.

F. The Snap Pixel

167. Defendant also installed code on the Website, created by Snapchat, that tracks Website users' actions, behavior, and conversions across the Website (the "Snap Pixel").

168. To make use of the Snap Pixel, Defendant must create a Snapchat Ads manager account, create a pixel, receive a Pixel ID, select the information to be collected, follow specific guides for integration with third-party software like Spotify or Google Tag Manager, and determine whether to enable automated matching for the Snap Pixel.[109]

169. The Snap Pixel is a piece of JavaScript code provided by Snapchat that allows advertisers, such as Defendant, to track user actions and behavior on websites for the purpose of measuring ad performance, optimizing ad campaigns, and building targeted audiences for better advertising results.[110]

---

[108] *Id.*

[109] *Getting Started with Enabling the Pixel*, SNAPCHAT, https://businesshelp.snapchat.com/s/article/pixel-website-install?language=en_US&r=692&ui-knowledge-components-aura-actions.KnowledgeArticleVersionCreateDraftFromOnlineAction.createDraftFromOnlineArticle=1 (last visited Dec. 22, 2025).

[110] *Using the Snap Pixel*, SNAPCHAT (July 11, 2023) https://forbusiness.snapchat.com/blog/the-snap-pixel-how-it-works-and-how-to-install-it (last visited Dec. 22, 2025); *see also Snapchat Pixels*, SPRINKLR, https://www.sprinklr.com/help/articles/snapchat-pixel/snapchat-pixels/640739d87517d84a3aaf2d26 (last visited October 09, 2025); Marialuisa Aldeghi, *How to set up the Snap Pixel: A step-by-step guide*, LEADSBRIDGE (Dec. 18, 2024), https://leadsbridge.com/blog/snap-pixel/ (last visited Dec. 22, 2025).

170. "For the Pixel to work, [Snapchat] must receive a Pixel ID and a standard event type[,]" at a minimum.[111]

171. The Pixel ID is an "[a]dvertiser specific ID . . ."[112] where the Pixel ID is used to initialize the Snap Pixel's tracking,[113] identifying which advertising account receives the collected data.

172. This software may be added automatically or manually to a website's pages, but in either case, it must be added to each webpage being tracked.[114]

173. Key features of the Snap Pixel include tracking user actions ("events") designated by advertisers, such as page views, add-to-cart actions, purchases, and sign-ups.[115] Advertisers, such as Defendant, can add additional parameters to these events for more granular insights, like purchase value or product type information.[116] The information is collected immediately as users land on the website where the pixel is installed. [117]

. The Snap Pixel also allows cross-device tracking, enabling tracking across multiple devices to provide a comprehensive view of a customer's journey.[118]

---

[111] Snap Pixel FAQ, SNAPCHAT, https://businesshelp.snapchat.com/s/article/snap-pixel-faq?language=en_US (last visited Dec. 22, 2025).
[112] *Snap Pixel Helper Glossary*, SNAPCHAT, https://businesshelp.snapchat.com/s/article/pixel-helper-glossary?language=en_US (last visited Dec. 22, 2025)
[113] *See About Snap Pixel*, SNAPCHAT, https://businesshelp.snapchat.com/s/article/snap-pixel-about?language=en_US (last visited Dec. 22, 2025)
[114] *See Directly Implement the Pixel On Your Website*, SNAPCHAT, https://businesshelp.snapchat.com/s/article/pixel-direct-implementation?language=en_US (last visited Dec. 22, 2025).
[115] *Pixel Event Examples*, SNAPCHAT, https://businesshelp.snapchat.com/s/topic/0TO8b000000P8xxGAC/pixel-event-examples?language=en_US (last visited Dec. 22, 2025).
[116] *Additional Parameters Example*, SNAPCHAT, https://businesshelp.snapchat.com/s/article/additional-parameters?language=en_US (last visited Dec. 22, 2025).
[117] *Using the Snap Pixel*, SNAPCHAT (July 11, 2023), https://forbusiness.snapchat.com/blog/the-snap-pixel-how-it-works-and-how-to-install-it (last visited Dec. 22, 2025); *see also* Marialuisa Aldeghi, *How to set up the Snap Pixel: A step-by-step guide*, LEADSBRIDGE (Dec. 18, 2024) https://leadsbridge.com/blog/snap-pixel/ (last visited Dec. 22, 2025).
[118] *About Snap Pixel*, SNAPCHAT, https://businesshelp.snapchat.com/s/article/snap-pixel-about?language=en_US#:~:text=The%20Snap%20Pixel%20is%20a,to%20manage%20your%20privacy%20settings (last visited Dec. 22, 2025).

175. The Snap Pixel collects:

a. The time the website actions occurred;[119]

b. Device information such as the hardware model, operating system, and browser type used;[120]

c. Cookies;[121]

d. Metadata such as button clicks, time spent on the site, conversations, and page visits;[122] and

e. IP addresses for general geographic data.[123]

176. The Snap Pixel enables website owners, such as Defendant, to understand how users navigate to their site. This data helps Defendant refine their advertising strategies by identifying high-performing campaigns and optimizing ad spending.[124]

177. The Website's Snap initialization code and Pixel event activations transmit Defendant's Pixel ID in the form of a URL parameter named "pid," which contains Defendant's Snap Pixel ID value of "15913fc5-6301-4257-a1e1-7714317d1346." This data is sent both when the Website receives communications and when users send communications to the Website.

178. The information the Snap Pixel collects provides Defendant with a better understanding of who its customers are and how they navigate around the Website.

---

[119] *Snap Pixel: Power Your Ad Performance*, SNAPCHAT, https://forbusiness.snapchat.com/advertising/snap-pixel (last visited Dec. 22, 2025).
[120] *Privacy Policy*, SNAP (Apr. 21, 2025) https://values.snap.com/privacy/privacy-policy (last visited Dec. 22, 2025).
[121] *Cookie information*, SNAP (Apr. 8, 2025), https://www.snap.com/privacy/cookie-information (last visited Dec. 22, 2025).
[122] Ate Keurentjes, *How do you install the Snap Pixel via Google Tag Manager*, TAGGRS (Oct. 23, 2025) https://taggrs.io/en/snap-pixel/ (last visited Dec. 22, 2025).
[123] *Directly Implement the Pixel On Your Website*, SNAPCHAT, https://businesshelp.snapchat.com/s/article/pixel-direct-implementation?language=en_US (last visited Dec. 22, 2025); *see also Privacy Policy*, SNAP (Apr. 21, 2025), https://values.snap.com/privacy/privacy-policy (last visited Dec. 22, 2025); *Data Processing* Agreement, SNAP (July 25, 2025), https://www.snap.com/terms/data-processing-agreement (last visited Dec. 22, 2025).
[124] Aldeghi, *supra* note 2.

179. Snap also benefits from non-customer-list audience information independently.[125]

180. The harvested data collected by the Snap Pixel is used by Defendant to create custom audiences.[126] Defendant can retarget users who viewed specific pages or made purchases and build lookalike audiences to reach new users with similar characteristics.[127]

181. Put simply, the Snap Pixel collects as much data as possible about otherwise anonymous users of the Website and matches it with existing data that Snapchat has acquired and accumulated about millions of Americans to improve Defendant's conversion rates and reduce overall advertising costs.

182. Snap Pixel requires advertisers, such as Defendant, to integrate code into their website's header or use tools like Google Tag Manager for a seamless setup.[128] Advertisers, such as Defendant, are encouraged to use tools like Snap Pixel Helper to verify proper installation, ensure accurate event tracking, and track user activity.[129]

183. Defendant, through the Snap Pixel, uses data and cookies to track users and serve them relevant ads on Snapchat based on their interactions with the Website.[130] The data received from Snapchat conversion tracking allows Defendant to serve highly targeted ad campaigns to the right people.[131]

184. Using Snap Pixel helps Defendant collect important information about the people who buy from them, so Defendant can, in turn, benefit. Here are some of the biggest benefits:

---

[125] *See Privacy Policy*, *Section 2(g),* SNAP (Apr. 21, 2025) https://values.snap.com/privacy/privacy-policy (last visited Dec. 22, 2025).
[126] Aldeghi, *supra* note 2.
[127] *Id.*
[128] *Id.*
[129] *Snap Pixel: Power Your Ad Performance*, SNAPCHAT, https://forbusiness.snapchat.com/advertising/snap-pixel (last visited Dec. 22, 2025).
[130] *Id.*
[131] *Id.*

a. **Measure conversion events that matter**: See all the actions users take on the Website, across all devices, and attribute conversions back to ad campaigns.

b. **Reach the perfect audience**: Defendant can create custom audiences and lookalike audiences based on the specific actions users have taken on the Website.

c. **Optimize advertising campaigns**: Use real-time insights to optimize delivery of Defendant's campaigns for more effective results.[132]

185. An image of the invasive Snap Pixel code secretly embedded on Defendant's Website can be seen here:

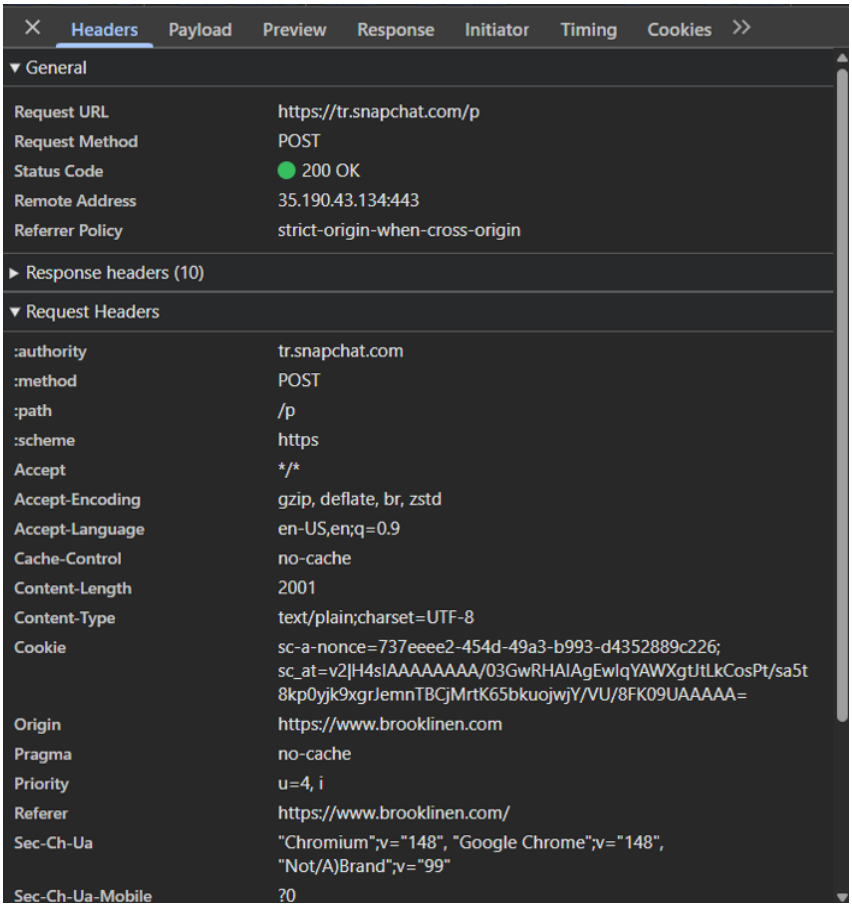


Figure 36 – Snap Pixel active on the Website

[132] *Benefits of Using the Snap Pixel*, SNAPCHAT, https://forbusiness.snapchat.com/blog/the-snap-pixel-how-it-works-and-how-to-install-it (last visited Dec. 22, 2025).

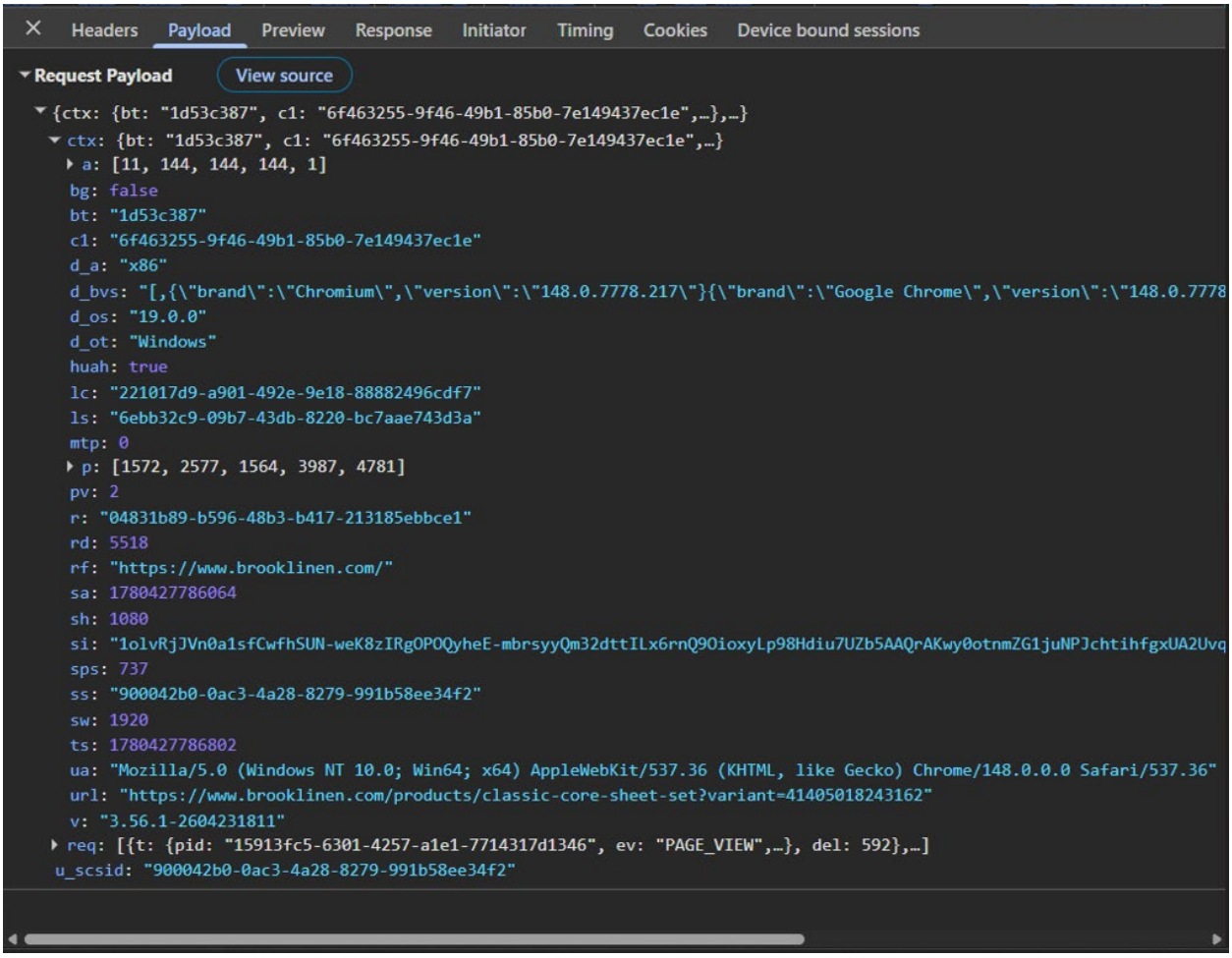


Figure 37 – Information intercepted by the Snap Pixel on the Website

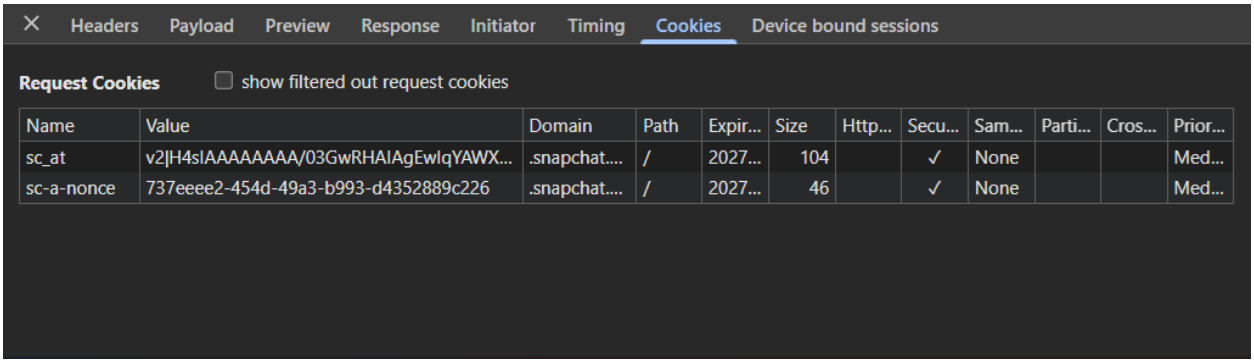


Figure 38 – Cookies transmitted by the Snap Pixel on the Website

186. When the Snap Pixel triggers, it captures the relevant data and sends a transmission to Snapchat's servers, as depicted in the picture above, which shows Defendant's Snap Pixel instantly sending communications to Snapchat as users take certain actions on the Website, like

viewing a page.

187. By using the Snap Pixel and providing Snapchat with users' information, Defendant had to agree to Snapchat's Personal Data Terms (the "Snap Terms"), among other agreements governing the use of the Snap Pixel.

188. By agreeing to the Snap Terms, Defendant represented and warranted that the personal data it shares with Snapchat will not contain any information about individuals under the age of 13 or any sensitive information or special category data.[133]

189. The Snap Terms further require Snap Pixel users, such as Defendant, of their responsibility to secure and maintain "all necessary rights, licenses and consents required to provide or make available the personal data" shared through the Snap Pixel.[134]

190. As a sophisticated party entering into a business arrangement with another sophisticated party, Defendant was on notice of the potential privacy violations that would result from the use of the Snap Pixel, and ignored Snapchat's warnings to safely handle its users' data and to warn its users that the Website would disclose their information in a manner that threatens their private information.

V. Defendant's Conduct Violated the Federal Wiretap Act and CIPA

191. Courts analyze claims under Cal. Penal Code § 631 under the same framework applied to claims under the federal Wiretap Act. *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020).

192. Cal. Penal Code § 631(a) prohibits several distinct and independent forms of unlawful interception, including: (1) intentionally tapping or making an unauthorized connection

[133] *Personal Data Terms*, SNAP (Dec. 9, 2024) https://www.snap.com/terms/personal-data#:~:text=In%20summary%3A%20you%20provide%20a,information%3B%20you%20obtained%20any%20necessary (last visited Dec. 22, 2025).
[134] *Id.*

with a communication; (2) willfully attempting to read or learn the contents or meaning of a communication while it is in transit; and (3) using or communicating information obtained through such interception. Section 631(a)(iv) separately imposes liability on any party who aids, agrees with, employs, or conspires with another to commit any of those acts.

193. Similarly, the federal Wiretap Act prohibits the intentional interception[135] of any wire, oral, or electronic communication without the consent of at least one authorized party to the communication. *See* 18 U.S.C. § 2511.

A. The Tracking Entities Intercepted the Contents of Communications Between Users and the Website in Transit

194. Transmitted URLs that include both the path and query string reflect the substance of a user's communication and therefore constitute content.

195. Here, the network requests intercepted by the Tracking Entities included detailed Request URLs created by Defendant containing the names and file locations of webpages, the detailed URLs and content users requested and accessed on the Website, identifying information in the form of cookies, and users' activity information reflecting their interactions with the Website.

196. The Tracking Tools intercepted the contents of Plaintiff's communications contemporaneously with Plaintiff's interactions with the Website. The Tracking Tools began transmitting data to the Tracking Entities as soon as the Tracking Tools loaded onto Plaintiff's browsers, and additionally transmit data at the moment Plaintiff submitted information through the Website.

[135] "[I]ntercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

197. This interception, duplication, and transmission occurred inside Plaintiff's browsers, before the communications fully reached users' devices, or otherwise before the communications were transmitted from users' devices, and therefore occurred while the communications were in transit.

198. The Tracking Entities were third parties to Plaintiff's communications with Defendant, and intercepted, read, duplicated, and retransmitted users' data while it was in transit.

199. Defendant's deployment of the Tracking Tools enabled Tracking Entities to intercept Request URLs that specified the content Plaintiff accessed on the Website, in violation of CIPA at Cal. Penal Code § 631 and the federal Wiretap Act at 18 U.S.C. § 2511(1)(a).

B. Defendant Procured Tracking Entities and Aided Tracking Tool Interceptions

200. A party violates Cal. Penal Code § 631 and 18 U.S.C. § 2511(1) not only by directly intercepting communications, but also by knowingly permitting, procuring, or facilitating third-party interception. *See Yoon v. Lululemon USA, Inc.,* 549 F. Supp. 3d 1073, 1083 (C.D. Cal. 2021) ("[A] conversationalist is betrayed equally by a wiretapper and by the willing conversation participant who surreptitiously allows that third party to wiretap.").

201. Defendant knowingly procured the Tracking Entities to embed and configure the Tracking Tools in its Website, in a manner that enabled the Tracking Entities to intercept the contents of Plaintiff's communications with the Website.

202. CIPA at Cal. Penal Code § 631(a) requires the prior consent of all parties to the communication.

203. The Federal Wiretap Act at 18 U.S.C. § 2511(2)(d) requires the prior consent of at least one party to the communication.

204. Defendant did not obtain Plaintiff's express or implied consent to allow the Tracking Entities to intercept those communications, before or after the interceptions occurred, nor could Defendant consent to the interception of those communications, as the scope of its consent was bound to the Terms provided by the Tracking Entities, which required obtaining valid prior consent from Plaintiff and/or otherwise prohibited the use of the Tracking Tools for intercepting sensitive or legally protected data.

C. The Tracking Tools are Trap and Trace and/or Pen Register Devices

205. California law defines a "trap and trace device" as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

206. California law defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

207. The Tracking Tools are processes to identify the source of electronic communication by capturing incoming electronic impulses and identifying dialing, routing, addressing, and signaling information generated by users, who are never informed that the website is collaborating with the Tracking Entities to obtain their phone number and other identifying information. As such, the Tracking Tools are "trap and trace" devices.

208. Defendant is a "provider of electronic or wire communication service" because it provides the Website, where users send electronic communications. Cal. Penal Code § 638.51(b).

209. The Tracking Tools are "reasonably likely" to identify the source of incoming electronic impulses, as well as record the routing and addressing information. In fact, they are designed specifically for that purpose. The IP addresses, detailed URLs, cookies, and Google IDs disclosed through the use of the Tracking Tools identify: (i) the source and destination of incoming signals to Plaintiff's devices to the Tracking Entities; and (ii) the source and destination of outgoing signals from Plaintiff's devices.

210. Defendant did not obtain Plaintiff's express or implied consent to be subjected to data sharing with the Tracking Tools for the purposes of digital fingerprinting and de-anonymization.

211. CIPA at California Pen. Code § 637.2 imposes civil liability and statutory penalties for the installation of trap and trace software without a court order. No court order to install a trap and trace device via the Tracking Tools was obtained by Defendant.

212. Defendant did not obtain Plaintiff's or the Class members' express or implied consent to be subjected to data sharing with the Tracking Entities for the purposes of fingerprinting and de-anonymization, nor did Defendant obtain a court order.

D. Defendant Promised Users that Tracking Could Be Disabled, but Continued Tracking Anyway

213. When users visit Defendant's Website, they are presented with a Cookie Banner and Cookie Settings that state that users can decline all non-necessary cookies, including those from the Tracking Entities.

214. The Cookie Settings provides toggles and controls that allow users to decline cookies that are not required for the Website to function.

215. Users who decline data sharing reasonably believe that non-necessary cookies will stop. The Cookie Settings communicate that users can prevent their browsing activity from being shared with Tracking Entities through the use of cookies.

216. These representations are false.

217. Even after users declined non-necessary cookies, Defendant continued deploying Tracking Tools that intercepted users' interactions with the Website and transmitted those communications and identifiers to third-party tracking companies via cookies.

218. Users were told they could disable tracking, attempted to do so, and the Defendant continued tracking them regardless.

E. Defendant Lacked Consent and Misrepresented the Effectiveness of Cookie Settings

219. Plaintiff's investigation revealed that the Website's default settings permitted tracking to begin as soon as users arrived on the Website, before users could make any choices on the Cookie Banner.

220. As a result, users were tracked from the moment they began using the Website, without prior consent.

221. Plaintiff visited the Website while those default tracking settings were active.

222. Users who visit the Website are shown a Cookie Banner that offers the option to affirmatively reject non-necessary cookies and to modify cookie preferences.

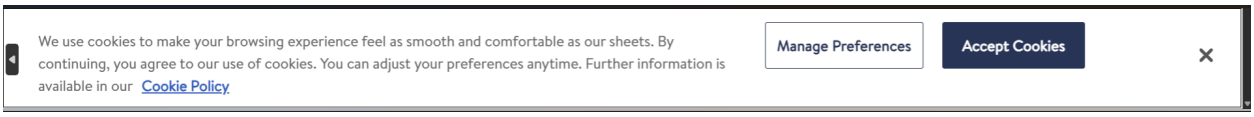


Figure 39 – The Cookie Banner shown to users who visit the Website

223. Despite those representations, users who declined all non-necessary cookies were still tracked by at least Meta, TikTok, Microsoft, Google PageAd, Google Analytics, Reddit, Pinterest, and Snapchat through the use of cookies.

224. Defendant intentionally shared Plaintiff's and users' Sensitive Information with the Tracking Entities, placed TikTok, Meta, Google, Microsoft, Pinterest, Reddit and Snapchat tracking cookies on the Website, and allowed the Tracking Entities to track users and intercept their communications with the Website, despite stating in the Cookie Banner that Tracking Tools such as cookies would not be placed if users rejected the use of non-necessary cookies.

225. Defendant placed and permitted the Tracking Entities to place identifying cookies. These cookies identify users and allow the Tracking Entities to track users, intercept their communications, and build personal profiles based on that tracking.

226. Representations regarding cookie-consent controls are materially misleading where tracking continues despite a website's claim to the contrary and/or users' selections.

227. Defendant and the Tracking Entities benefited from the interception of Plaintiff's communications by reading and subsequently using the intercepted contents to construct detailed profiles reflecting Plaintiff's browsing habits and interests, and by using those profiles for targeted advertising.[136]

228. The Tracking Entities independently benefit from intercepting communications, using data collected through the Tracking Tools to improve their advertising products and market those capabilities to other businesses.[137]

---

[136] *[GA4] User Explorer* GOOGLE, https://support.google.com/analytics/answer/9283607?sjid=14886665613386572022-NA#zippy=%2Cin-this-article (last visited May 7, 2026).

[137] *See Data sharing settings*, GOOGLE https://support.google.com/analytics/answer/1011397?hl=en&ref_topic=2919631&sjid=14886665613386572022-NA (last visited May 7, 2026).

CLASS ALLEGATIONS

229. Plaintiff brings these claims for relief pursuant to the Federal Rules of Civil Procedure 23(a), 23(b)(2), or 23(b)(3) on behalf of the following Class and Subclasses (collectively "the Class").

230. Plaintiff brings this class action individually and on behalf of the following Class:

> All natural persons who visited Defendant's Website in the United States during the applicable limitations period, who interacted with the Website's Cookie Banner and/or Cookie Settings and rejected the Website's use of Tracking Tools, and whose electronic communications were intercepted, disclosed, and/or transmitted to the Tracking Entities through Defendant's use of the Tracking Tools (the "Class").

231. Plaintiff brings this class action individually and on behalf of the following California Subclass:

> All members of the Class who visited and interacted with the Defendant's Website during the applicable limitations period while located in the State of California (the "California Subclass").

232. Specifically excluded from the Class are Defendant, Defendant's officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, servants, partners, joint venturers, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

233. Plaintiff reserves the right to amend the Class and Subclasses definitions above if further investigation and/or discovery reveal that the Class should be expanded, narrowed, further divided into subclasses, or otherwise modified in any way.

234. NUMEROSITY: At this time, Plaintiff does not know the number of Class members but believes the number to be at least measured in thousands, if not millions, given the popularity of Defendant's Website. The number of persons within the Class is believed to be so

numerous that joinder of all members is impractical. The exact identities of Class members may be ascertained via the records maintained by the Defendant in the ordinary course of its business.

235. COMMONALITY: Common questions of fact and law exist as to all Class members and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between the Class members, and which may be determined without reference to the individual circumstances of any Class member, include but are not limited to the following:

a. Whether Defendant shared the Class members' Sensitive Information with the Tracking Entities or other third parties and/or facilitated the Tracking Entities' interception of the Class members' Sensitive Information;

b. Whether Defendant obtained effective and informed consent to do so;

c. Whether Defendant's conduct constitutes a violation of the Wiretap Act;

d. Whether the Class members are entitled to actual damages, punitive damages, and/or statutory penalties; and

e. Whether the Class members are entitled to injunctive relief.

236. TYPICALITY: As persons who visited Defendant's Website and whose personal information was shared by Defendant, Plaintiff is asserting claims that are typical of the Class members.

237. ADEQUACY: Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained attorneys experienced in class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the Class members or whose inclusion would otherwise be improper are excluded.

238. SUPERIORITY: A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class members is impracticable and inefficient. It would be unduly burdensome on the courts, where individual litigation of numerous cases would proceed. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for their wrongdoing as asserted herein.

CAUSES OF ACTION

COUNT I
VIOLATIONS OF THE WIRETAP ACT 18 U.S.C. § 2510, et seq.
(On Behalf of Plaintiff and the Class)

239. Plaintiff incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

240. Plaintiff brings this cause of action on behalf of herself and all Class members.

241. The federal Wiretap Act prohibits the intentional interception of any wire, oral, or electronic communication without the consent of at least one authorized party to the communication. *See* 18 U.S.C. § 2511.

242. The Wiretap Act provides a private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

243. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

244. The Wiretap Act defines "contents" as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

245. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

246. The Wiretap Act defines "person" to include any individual, partnership, association, trust, or corporation. 18 U.S.C. § 2510(6).

247. Plaintiff, Defendant, and the Tracking Entities are "persons" within the meaning of the Wiretap Act.

248. The Tracking Tools, Plaintiff's devices and browsers, and Defendant's Website server constitute "device[s]" or "apparatus[es]" capable of intercepting wire, oral, or electronic communications within the meaning of 18 U.S.C. § 2510(5).

249. Plaintiff had a reasonable expectation of privacy in her electronic communications with Defendant's Website, including the pages she viewed, browsing activity, and other interactions with Website features, particularly where Defendant represented through its Cookie Banner and Cookie Settings that users could reject non-necessary cookies.

250. Within the relevant time period, Plaintiff's electronic communications with the Website were intercepted contemporaneously at the moment they were collected by the Tracking Tools and transmitted to Tracking Entities without Plaintiff's consent from Plaintiff's browser, for the unlawful purpose of monetizing the Plaintiff's intercepted information, including for combining that information with information collected about Plaintiff from across the Internet via the same Tracking Tools and used for advertising, analytics, and marketing optimization.

251. Interception occurred whenever Plaintiff interacted with the Website, including when she navigated webpages, viewed content, or otherwise communicated information to the Website through her browser.

252. At all relevant times, Defendant's conduct was knowing, willful, and intentional. Defendant is a sophisticated commercial entity that knowingly embedded and enabled the Tracking Tools on its Website and understood that doing so would result in the interception and transmission of users' communications to the Tracking Entities.

253. Plaintiff did not consent to the interception, recording, disclosure, or use of her electronic communications with the Website by the Tracking Entities. On the contrary, Plaintiff affirmatively declined Tracking Entities' tracking through Defendant's Cookie Banner and Cookie Settings.

254. The unauthorized interception and use of Plaintiff's electronic communications by the Tracking Entities were only possible because Defendant knowingly and intentionally placed and enabled the Tracking Tools on the Website. 18 U.S.C. § 2511(1)(a).

255. As a direct and proximate result of Defendant's violations of the Wiretap Act, Plaintiff has been damaged and is entitled to relief under 18 U.S.C. § 2520, including:

a. damages in an amount to be determined at trial, assessed as the greater of actual damages suffered by Plaintiff and any profits made by the intercepting parties as a result of the violations, or

b. statutory damages of the greater of $100 per day per violation or $10,000; appropriate equitable and declaratory relief; and

c. reasonable attorneys' fees and costs.

COUNT II
INVASION OF PRIVACY AND
VIOLATIONS OF THE CALIFORNIA CONSTITUTION, Art. 1, § 1
(On Behalf of Plaintiff Gilbert and the California Subclass)

256. Plaintiff Gilbert incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

257. Plaintiff Gilbert brings this cause of action on behalf of herself and all California Subclass members.

258. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

259. California voters added the word "and privacy" to the California Constitution when they passed Proposition 11 in 1972. Proposition 11 is also known as the "Privacy Initiative" or "Right to Privacy Initiative." In support of Proposition 11, voters stated that the right of privacy is the right to be left alone… It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control the circulation of personal information. This is essential to social relationships and personal freedom. Plaintiff Gilbert and the California Subclass members have a legally protected interest in their Sensitive Information, such as browsing activity, device identifiers, and related metadata, which Defendant violated by providing the Tracking Entities access to that data, enabling the interception of such communications. Plaintiff Gilbert and California Subclass members' protected interests arise from various statutes and common law, including, *inter alia*, the Wiretap Act, the CIPA, and the California Constitution, which protects privacy rights and

includes the "ability to control circulation of our personal information." The privacy rights of Plaintiff Gilbert and the California Subclass members were invaded through the interception and collection of their data, which included their Sensitive Information and other sensitive information, without first obtaining authorization or consent from Plaintiff Gilbert and the California Subclass members. Plaintiff Gilbert and the California Subclass members had a reasonable expectation of privacy when communicating with Defendant's Website and thereby providing and/or transmitting their Sensitive Information. By causing third-party cookies and Tracking Entities to be placed on users' browsers and devices and by transmitting users' Sensitive Information to Tracking Entities despite users' selections, Defendant violated their reasonable expectation of privacy.

260. Defendant's intrusion, placing third-party Tracking Tools and enabling third-party access to users' Sensitive Information despite users' express rejection of such tracking, is and would be highly offensive to a reasonable person.

261. As a direct and proximate result of Defendant's intentional invasion of their privacy rights, Plaintiff Gilbert and the California Subclass members have been harmed and are entitled to compensatory, punitive, and injunctive relief.

COUNT III
VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 631
(On Behalf of Plaintiff Gilbert and the California Subclass)

262. Plaintiff Gilbert incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

263. Plaintiff Gilbert brings this cause of action on behalf of herself and all California Subclass members.

264. CIPA was enacted to curb "the invasion of privacy resulting from the continual and increasing use of" certain technologies determined to pose "a serious threat to the free exercise of personal liberties." CIPA extends civil liability for various surveillance technologies.

265. CIPA provides that a person is liable to another where, "by means of any machine, instrument, contrivance, or in any other manner," committed any of the following: (i) intentionally tapped, or made any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, cable, or instrument of any internal telephonic communication system; or (ii) willfully and without consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or 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 being sent from or received at any place within this state; or (iii) uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; or (iv) 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. Cal. Penal Code § 631(a).

266. The Ninth Circuit has confirmed that one of the purposes of wiretapping statutes is to "prevent the acquisition of the contents of a message by an unauthorized third-party . . . ." *In re Facebook Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020). In dealing specifically with CIPA, the California Supreme Court has similarly concluded that the objective of CIPA is to protect a person's communications "from a situation where the other person on the other end of the line permits an outsider" to monitor the communication. *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985); *see also Smith v. LoanMe*, 11 Cal. 5th 183, 200 (2021).

267. Further, the California Supreme Court has explained the legislative purpose behind CIPA, holding that "secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements." *Ribas*, 38 Cal. 3d at 360-61. The Court recognized a substantial distinction between the secondhand repetition of a conversation and its "simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device." *Id*.

268. The Website, the Tracking Tools, and Plaintiff Gilbert's devices and browsers each qualify as a "machine, instrument, contrivance, or . . . other manner" used to engage in the prohibited conduct at issue here. *See* Cal. Penal Code § 631(a).

269. Within the relevant time period, the Tracking Entities, including Google, through the use of the Tracking Tools, without the consent of all parties to the communication, or in any unauthorized manner, willfully read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff Gilbert and the California Subclass members, contemporaneous with the communications transit through or passing over any wire, line or cable or with the communications sending from or being received at any place within California. The information collected by the Tracking Tools was not for the sole benefit of Defendant.

270. Within the relevant time period, Defendant aided, agreed with, and employed the Tracking Entities to accomplish the wrongful conduct at issue here.

271. Plaintiff Gilbert and the California Subclass members did not authorize or consent to the tracking, interception, and collection of any of their electronic communications. Defendant's violations of Cal. Penal Code § 631 constitute invasions of privacy of Plaintiff Gilbert and the California Subclass members' respective rights to privacy.

COUNT IV
VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 638.51
(On Behalf of Plaintiff Gilbert and the California Subclass)

272. Plaintiff Gilbert incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

273. Plaintiff Gilbert brings this cause of action on behalf of herself and all California Subclass members.

274. California's Pen Register and Trap and Trace Law is part of CIPA, codified at Cal. Penal Code §§ 630.50-638.55

275. A "pen register" is "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

276. A "trap and trace device" is "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably. "Process" includes "software that identifies consumers, gathers data, and correlates that data through unique 'fingerprinting.'" *Greenley v. Kochava, Inc.*, 684 F.Supp.3d 1024, 1050 (S.D. Cal. 2023). Cal. Penal Code § 638.51(a) provides that "a person may not install or use a pen register or a trap and trace device without first obtaining a court order…." Defendant is "a provider of electronic or wire communication service" as they provide the Website, where users send electronic communications. Cal. Penal Code § 638.51(b). No court order to install pen register or trap and trace devices via the Tracking Tools was obtained by Defendant. Defendant uses pen register and trap and trace processes on its Website by deploying Tracking Tools designed to capture phone numbers, email addresses, routing

information, addresses, and other signaling information of website users. The Tracking Tools identify the source of the incoming electronic and wire communications to the Website.

277. Defendant was not authorized by any court order to use pen register or trap and trace devices to track Plaintiff Gilbert and the California Subclass members' activity on the Web. Defendant did not obtain consent from Plaintiff Gilbert or the California Subclass members before using pen register or trap and trace technology to identify users of its Website, and has violated Section 638.51. As a direct and proximate result of Defendant's conduct, Plaintiff Gilbert and the California Subclass members suffered losses and were damaged in an amount to be determined at trial. CIPA imposes civil liability and statutory penalties for violations of Cal. Penal Code § 638.51.

COUNT V
VIOLATIONS OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code § 1770, et seq.
(On Behalf of Plaintiff Gilbert and the California Subclass)

278. Plaintiff Gilbert incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

279. Plaintiff Gilbert brings this cause of action on behalf of herself and all California Subclass members.

280. The CLRA prohibits any person from undertaking any "unfair methods of competition and unfair or deceptive acts or practices" in a transaction "that results in the sale or lease of goods or services to any consumer."

281. Defendant is a person within the meaning of the CLRA.

282. Plaintiff Gilbert is a consumer of Defendant's services under the CLRA, as Plaintiff Gilbert used Defendant's Website to browse for information.

283. Defendant undertook deceptive acts or practices in violation of the CLRA by failing to disclose the presence of the Tracking Tools on the Website. Defendant violated Cal. Civ. Code § 1770(a)(2) by "[m]isrepresenting the source, sponsorship, approval, or certification of goods or services."

284. By this failure to disclose, Defendant violated Cal. Civ. Code § 1770(a)(5) by "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

285. By this failure to disclose, Defendant violated Cal. Civ. Code § 1770(a)(14) by "[r]epresenting that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law."

286. Defendant's failure to disclose was material to Website users, such as Plaintiff Gilbert. Users could have chosen a different website that did not use Tracking Tools, chosen a website that disclosed the presence of Tracking Tools and allowed them to be disabled, and/or chosen a website that requested consent before implementing Tracking Tools.

287. Plaintiff Gilbert and California Subclass members seek all available relief for Defendant's use of unfair acts or practices, including injunctive relief.

COUNT VI
VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, et seq.
(On Behalf of Plaintiff Gilbert and the California Subclass)

288. Plaintiff Gilbert incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

289. Plaintiff Gilbert brings this cause of action on behalf of herself and all California Subclass members.

290. The UCL broadly prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice." *See* Cal. Bus. & Prof. Code § 17200.

291. By actively and affirmatively misleading consumers by omitting to inform them of the Tracking Tools on the Website, Defendant has violated the unlawful prong of the UCL.

292. Defendant has violated the unlawful prong of the UCL by way of Defendant's above-described violations of the Wiretap Act, CIPA, and the FSCA arising from Defendant's purposeful installation and utilization of the Tracking Tools on the Website.

293. By actively and fraudulently deceiving users about their ability to disable the Tracking Tools, Defendant has violated the unlawful prong of the UCL.

294. Defendant failed to disclose the presence of the Tracking Tools on the Website. Defendant disclosed Plaintiff Gilbert's and the California Subclass members' Sensitive Information without their knowledge or consent. Defendant disclosed Plaintiff Gilbert's and the California Subclass members' information to the Tracking Entities to build personal profiles without their knowledge or consent. Defendant failed to disclose that it was wiretapping users' communications with the Website. Defendant fraudulently deceived users about their ability to disable the Tracking Tools. Through this conduct, Defendant violated the UCL's unfair prong.

295. Plaintiff Gilbert has standing to bring claims against Defendant under the UCL. Plaintiff Gilbert's information was tracked and recorded without consent. Plaintiff Gilbert's data was used to build personal profiles for advertising purposes without consent.

296. Plaintiff Gilbert would have considered it important to the decision to visit Defendant's Website to learn that her data was being tracked and recorded without her consent, regardless of privacy settings made through the Cookie Banner and Cookie Settings.

297. Instead, Plaintiff Gilbert exercised the Website's privacy controls and continued using the Website in reliance on Defendant's representations that non-necessary cookies had been disabled.

298. Because of Defendant's UCL violations described above, Plaintiff Gilbert suffered injury by losing control of her personal data and having her Sensitive Information tracked and recorded without her consent.

299. Plaintiff Gilbert and California Subclass members seek all available relief for Defendant's use of unfair acts or practices, including injunctive relief.

COUNT VII
COMMON LAW FRAUD, DECEIT, AND/OR MISREPRESENTATION
(On Behalf of Plaintiff and the Class)

300. Plaintiff incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

301. Plaintiff brings this cause of action on behalf of herself and all Class members.

302. Defendant made affirmative representations to users through its Cookie Banner, Cookie Settings, and related disclosures that users could decline all non-essential cookies.

303. Defendant represented that exercising those options would limit or prevent the deployment of Tracking Tools, including analytics and marketing cookies, and would stop the transmission of users' browsing activity, interactions, and related data to the Tracking Entities.

304. Defendant made these representations at the time users first accessed the Website and again when users were prompted to review and confirm their cookie preferences.

305. Defendant knew the representations were false or misleading, or acted with reckless disregard for their truth, because Defendant controlled the Website's source code, selected and configured the Tracking Tools, and determined how those tools operated in relation to users' expressed privacy choices. Defendant also received reports on the Tracking Tools

functionality, which would have alerted them to decreased information intake if their "opt-in" Tracking Tool scheme was functioning as described.

306. Defendant had the technical ability to prevent data transmissions and to configure the Website so that non-essential tracking ceased when users declined such tracking. Industry-standard tools, configurations, and consent-management frameworks exist that permit websites to block, defer, or condition the loading of non-necessary cookies based on users' preferences, and Defendant could have implemented such measures.

307. Defendant made misrepresentations with the intent to induce reliance by users, including Plaintiff, by reassuring them that they could meaningfully control tracking while Defendant continued to collect and transmit data for its own commercial benefit.

308. Plaintiff and the Class members reasonably and justifiably relied on Defendant's misrepresentations by continuing to use the Website and by exercising the decline controls instead of avoiding the Website, withholding information, or taking additional steps to protect their privacy.

309. Plaintiff's and the Class members' reliance was reasonable because Defendant presented the Cookie Banner and Cookie Settings as mechanisms for exercising legally protected privacy rights and for controlling the collection and sharing of personal information.

310. As a direct and proximate result of Defendant's fraudulent conduct, Plaintiff and the Class members suffered damages, including loss of privacy, loss of control over their personal information, and diminution in the value of their personal data. Plaintiff and the Class members suffered injury, including unauthorized disclosure of their communications, loss of control over their personal information, and loss of the privacy protection Defendant represented it would provide.

311. Defendant's conduct also resulted in Defendant obtaining an unjust and improper benefit by continuing to collect, use, and monetize users' data despite representing that such practices would cease upon a user's decline.

312. Plaintiff and the Class members seek all available relief for Defendant's fraudulent conduct, including compensatory damages, restitution, disgorgement, punitive damages where available, and injunctive relief to prevent further misrepresentations.

COUNT VIII
NEGLIGENT MISREPRESENTATION
(On Behalf of Plaintiff and the Class)

313. Plaintiff incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

314. Plaintiff brings this cause of action on behalf of herself and all Class members.

315. Defendant misrepresented the effectiveness of the Cookie Banner and Cookie Settings on the Website. Defendant represented that Plaintiff could reject all non-necessary cookies using the Cookie Banner and Cookie Settings.

316. Even after Plaintiff chose to disable the sale or sharing of her personal information and rejected all non-necessary cookies, the Website continued to allow the Tracking Tools of the Tracking Entities to intercept Plaintiff's communications and place cookies on her devices.

317. Defendant was uniquely situated to provide information about the effectiveness of the Cookie Banner and Cookie Settings. Defendant designed and controlled the Website, including the implementation of the Cookie Banner, Cookie Settings, and Tracking Tools. Thus, Defendant owed a duty to Plaintiff to accurately represent the function of its Cookie Banner and Cookie Settings.

318. Defendant should have known that its representations regarding the effectiveness of the Cookie Banner and Cookies Settings were incorrect. Defendant owned and controlled the

Website and implemented the Cookie Banner, Cookie Settings, and Tracking Tools. Defendant should have known that the Cookie Banner and Cookie Settings did not disable or stop the placement of the Tracking Tools.

319. Plaintiff relied on Defendant's representations about the effectiveness of the Cookie Banner and Cookie Settings when using the Website. Plaintiff chose to disable the sale or sharing of her personal information and reject all non-necessary cookies, relying on Defendant's representation that this would prevent the sharing of her personal information with third parties.

320. Plaintiff reasonably relied on Defendant's representations regarding the effectiveness of the Cookie Banner and Cookie Settings, as Defendant owned and controlled the Website.

321. Defendant was aware that Plaintiff would rely on Defendant's representations regarding the effectiveness of the Cookie Banner and Cookie Settings. Defendant was the only party that possessed the information, authority, and expertise to inform users, such as the Plaintiff, about the effectiveness of the Cookie Banner and Cookie Settings.

322. Defendant's representations about the effectiveness of the Cookie Banner and Cookie Settings were made for the purpose of representing to users, such as the Plaintiff, that they could control their privacy on the Website and use the Website without their personal information being shared with third parties.

323. Plaintiff was damaged by the representations made by Defendant. Plaintiff lost control of her personal data, had the value of their personal data diminished, and was unjustly enriched by the Defendant due to the Defendant's misrepresentations.

COUNT IX
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

324. Plaintiff incorporates by reference and realleges each and every allegation set forth above in all preceding paragraphs of this Complaint.

325. Plaintiff brings this cause of action on behalf of herself and all Class members.

326. Defendant obtained a benefit by collecting, processing, and enabling third-party monetization of Plaintiff's and the Class members' Sensitive Information, which Defendant then used to increase the effectiveness of advertising, marketing, and sales and to generate revenue.

327. It is unjust that Defendant retains those benefits under circumstances in which the information was collected and transmitted in breach of the representations made to users and without valid consent.

328. Plaintiff and the Class members conferred these benefits on Defendant, and Defendant has been unjustly enriched at the expense of Plaintiff and the Class members. Equity and good conscience require restitution or disgorgement of the benefits unjustly retained by Defendant. Therefore, Plaintiff and the Class members are entitled to the relief set forth below.

PRAYER

WHEREFORE, Plaintiff individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

a. An order certifying the class and making all appropriate class management orders;

b. For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the respective Class and Subclasses and their counsel as Class Counsel;

c. For an order declaring the Defendant's conduct violates the statutes referenced herein;

d. For an order finding in favor of Plaintiff, the Class, and the California Subclass on all counts asserted herein;

e. Entry of an order for injunctive and declaratory relief as described herein, including, but not limited to, requiring Defendant to immediately (i) remove the Tracking Tools from the Website or (ii) add, and obtain, the appropriate consent from Website users;

f. An award of statutory damages or penalties to the extent available;

g. For damages in amounts to be determined by the Court and/or jury;

h. For pre-judgment interest on all amounts awarded;

i. For an order of restitution and all other forms of monetary relief;

j. An award of all reasonable attorneys' fees and costs; and

k. Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury of all issues so triable.

Dated: June 18, 2026

LEVI & KORSINSKY, LLP

By: */s/ Mark S. Reich*
Mark S. Reich (MR-4166)
Mark Jensen*
33 Whitehall Street, 27th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: mjensen@zlk.com

Counsel for Plaintiff and the Proposed Class

**pro hac vice* forthcoming