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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

KAREN EWART and BIANCA JOHNSTON, individuals on behalf of themselves, the general public, and those similarly situated,

Plaintiffs,

v.

FENDER MUSICAL INSTRUMENTS CORP.,

Defendant.

CASE NO.

CLASS ACTION COMPLAINT FOR INVASION OF PRIVACY; INTRUSION UPON SECLUSION; WIRETAPPING IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 631); USE OF A PEN REGISTER IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 638.51); COMMON LAW FRAUD, DECEIT AND/OR MISREPRESENTATION; AND UNJUST ENRICHMENT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiffs Karen Ewart and Bianca Johnston ("Plaintiffs") bring this action on behalf of themselves, the general public, and all others similarly situated against Fender Musical Instruments Corp. ("Defendant" or "Fender"). Plaintiffs' allegations against Defendant are based on information and belief and the investigation of Plaintiffs' counsel, except for allegations specifically pertaining to Plaintiffs, which are based on their personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns egregious violations of consumer privacy and breach of consumer trust in violation of California law. When consumers visit Defendant's website (www.fender.com, the "Website"), Defendant displays to them a popup cookie consent banner. Defendant's cookie banner discloses that the Website uses cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendant assures visitors that they do not have to accept cookies—they can instead choose to decline or reject Defendant's use of cookies on the Website by selecting a "Do not sell my personal information" toggle switch, as shown in the following screenshot:

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

3. Even after users elect to decline or reject all cookies by adjusting the "Do not sell my personal information" toggle switch in the popup cookie consent banner, Defendant nonetheless caused multiple third parties—including Meta Platforms, Inc. (Facebook), Google LLC (YouTube, Google Play, and Google Analytics), ByteDance Ltd. (TikTok), Microsoft Corporation (Microsoft Bing and AppNexus), Adobe Inc. (demdex.net), Taboola, Inc., Live Ramp Holdings, Inc. (liadm.com), PubMatic, Inc., Magnite, Inc. (Rubicon Project), Criteo S.A.,

Index Exchange, Inc. (Casale Media), IPONWEB GmbH, Amazon.com, Inc., Pinterest, Inc., Reddit, Inc., TripleLift, Inc. (3lift.com), The Trade Desk, Inc. (adsrvr.org), Snap Inc. (SnapChat), Teads SA, and many others (the "Third Parties")—to place and/or transmit cookies that track users' website browsing activities and intercepted their private communications on the Website.

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

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

6. This type of tracking and data sharing is exactly what the Website visitors sought to avoid when they adjusted the "Do not sell my personal information" toggle switch on the Website's popup cookie consent banner. Defendant falsely told Website users that it respected their privacy choices and would refrain from tracking and data sharing when users declined or rejected cookies. Despite receiving clear notice of users' lack of consent, Defendant ignored those choices and violated state statutes and tort duties owed to Plaintiffs and those similarly situated Website users.

THE PARTIES

7. Plaintiff Karen Ewart is, and was at all relevant times, an individual and resident of Palo Alto, California. Plaintiff Ewart intends to remain in California and makes her permanent home there.

8. Plaintiff Bianca Johnston is, and was at all relevant times, an individual and resident of Big Bear City, California. Plaintiff Johnston intends to remain in California and makes her permanent home there.

9. Defendant Fender Musical Instruments Corp. is a Delaware corporation with its principal place of business in Los Angeles, California.

JURISDICTION AND VENUE

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

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

12. Further, the Private Communications and data that Defendant causes to be transmitted to Third Parties are routed through servers located in California.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in the state of California, including within this District.

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

FRAUDULENT CONCEALMEANT AND TOLLING

15. The delayed discovery rule applies to Plaintiffs' claims. Plaintiffs were unaware that, despite declining or rejecting all cookies by adjusting the "Do not sell my personal

information" toggle switch in the popup cookie consent banner on the Website, Defendant nonetheless caused third-party cookies to be sent to their browsers, stored on their devices, and transmitted to the Third Parties along with their private user data. Plaintiffs could not reasonably have discovered this conduct at the time of their visits to the Website because it occurred through hidden, technical processes not visible to ordinary users. Nothing about Plaintiffs' experiences on the Website would have alerted a reasonable user that their selections were not being honored. Plaintiffs lacked the technical expertise and specialized tools necessary to determine whether the Website honored their opt-out selections or instead continued transmitting their data notwithstanding their selections, and they did not discover Defendant's conduct until a later investigation revealed it.

16. On or about June 6, 2025, Plaintiff Johnston notified Defendant that it was engaging in the conduct alleged herein, including causing third-party cookies and corresponding user data to be stored on consumers' devices and transmitted to third parties despite users' rejection of all cookies that sell or share personal information. Despite this notice, Defendant did not disclose this conduct to users.

17. Despite exercising reasonable diligence, Plaintiffs were unaware of Defendant's conduct because Defendant affirmatively represented that users could decline or reject all cookies by adjusting the "Do not sell my personal information" toggle switch in the popup cookie consent banner, while simultaneously concealing that such tracking would occur regardless of users' selections. This combination of misrepresentation and omission prevented Plaintiffs from discovering their claims earlier. Defendant is not prejudiced by the timing of this action, as it has long been on notice of the conduct at issue, including through the June 6, 2025 demand letter describing substantially similar claims. These circumstances, including Defendant's concealment and misleading representations, warrant tolling of the statute of limitations.

SUBSTANTIVE ALLEGATIONS

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

18. Every website, including the Website, is hosted by a server that sends and receives communications in the form of HTTP requests, such as "GET" or "POST" requests, to and from Internet users' browsers. For example, when a user clicks on a hyperlink on the Website, the user's browser sends a "GET" request to the Website's server. The GET request tells the Website server what information is being requested (e.g., the URL of the webpage being requested) and instructs the Website's server to send the information back to the user (e.g., the content of the webpage being requested). When the Website server receives an HTTP request, it processes that request and sends back an HTTP response. The HTTP request includes the client's IP address, which allows the Website server to identify the origin of the request and return the response.

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

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

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

22. 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 server to a user's web browser and stored locally on the user's device. As described below, cookies generally contain a unique identifier which enables the website to recognize and differentiate individual users. Cookie files are sent back to the website server along with HTTP requests, enabling the website to identify the device making the requests, and to record a session showing how the user interacts with the website.

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

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

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

- **Browsing History**: Information about the webpages a Website user visits, including the URLs, titles, and keywords associated with the webpages viewed, time spent on each page, and navigation patterns;
- **Visit History**: Information about the frequency and total number of visits to the Website;

- **Website Interactions:** Data on which links, buttons, or ads on the Website that a user clicks;
- **User Input Data**: The information the user entered into the Website's form fields, including search queries, the user's name, age, gender, email address, location, and/or payment information;
- **Demographic Information**: Inferences about age, gender, and location based on browsing habits and interactions with Website content;
- **Interests and Preferences**: Insights into user interests based on the types of Website content viewed, products searched for, or topics engaged with;
- **Shopping Behavior**: Information about the Website products viewed or added to shopping carts;
- **Device Information**: Details about the Website user's device, such as the type of device (mobile, tablet, desktop), operating system, and browser type;
- **Referring URL**: Information about the website that referred the user to the Website;
- **Session Information**: Details about the user's current Website browsing session, including the exact date and time of the user's session, the session duration and actions taken on the Website during that session;
- **User Identifiers**: A unique ID that is used to recognize and track a specific Website user across different websites over time; and/or
- **Geolocation Data**: General location information based on the Website user's IP address or GPS data, if accessible, including whether the user is located in California.

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

26. Third-party cookies can be used for a variety of purposes, including (i) analytics (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing campaigns); (ii) personalization (e.g., remembering a user's browsing history and purchase

preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering targeted advertisements based on the user's consumer profile (i.e., an aggregated profile of the user's behavior, preferences, and demographics); and (iv) social media integration (e.g., enabling sharing of users' activities with social media platforms). Ultimately, third-party cookies are utilized to enhance website performance and generate revenue through data collection and targeted advertising.

27. Defendant manufactures, markets, and sells musical instruments, amplifiers, audio equipment, accessories, and related products under the Fender brand and affiliated brands. Defendant also owns and operates the Website, which allows visitors to, among other things, obtain information about Defendant's products, compare product features and specifications, access educational and support resources, locate dealers, and purchase products. As users interact with the Website—including by entering information into forms, searching for products or musical topics, viewing product specifications, comparing products, selecting options, clicking links, and navigating webpages—they communicate Private Communications to Defendant, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is located in California.

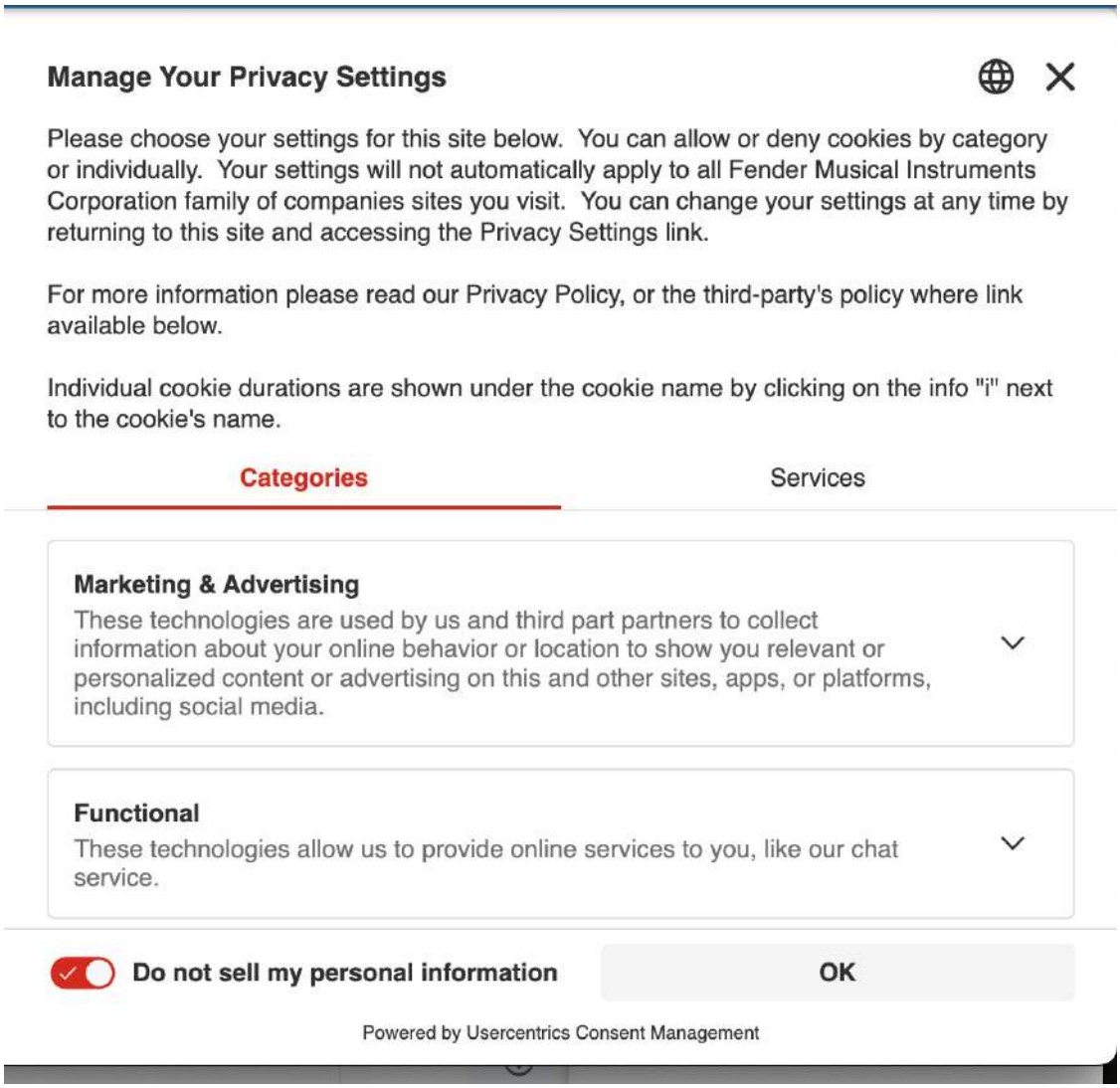
28. Defendant chose to install or integrate its Website with resources from the Third Parties that, among other things, use cookies. Thus, when consumers visit the Website, both first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is caused by software code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

29. Defendant explained the third-party cookies it used on the Website as follows in its Privacy Policy[1]:

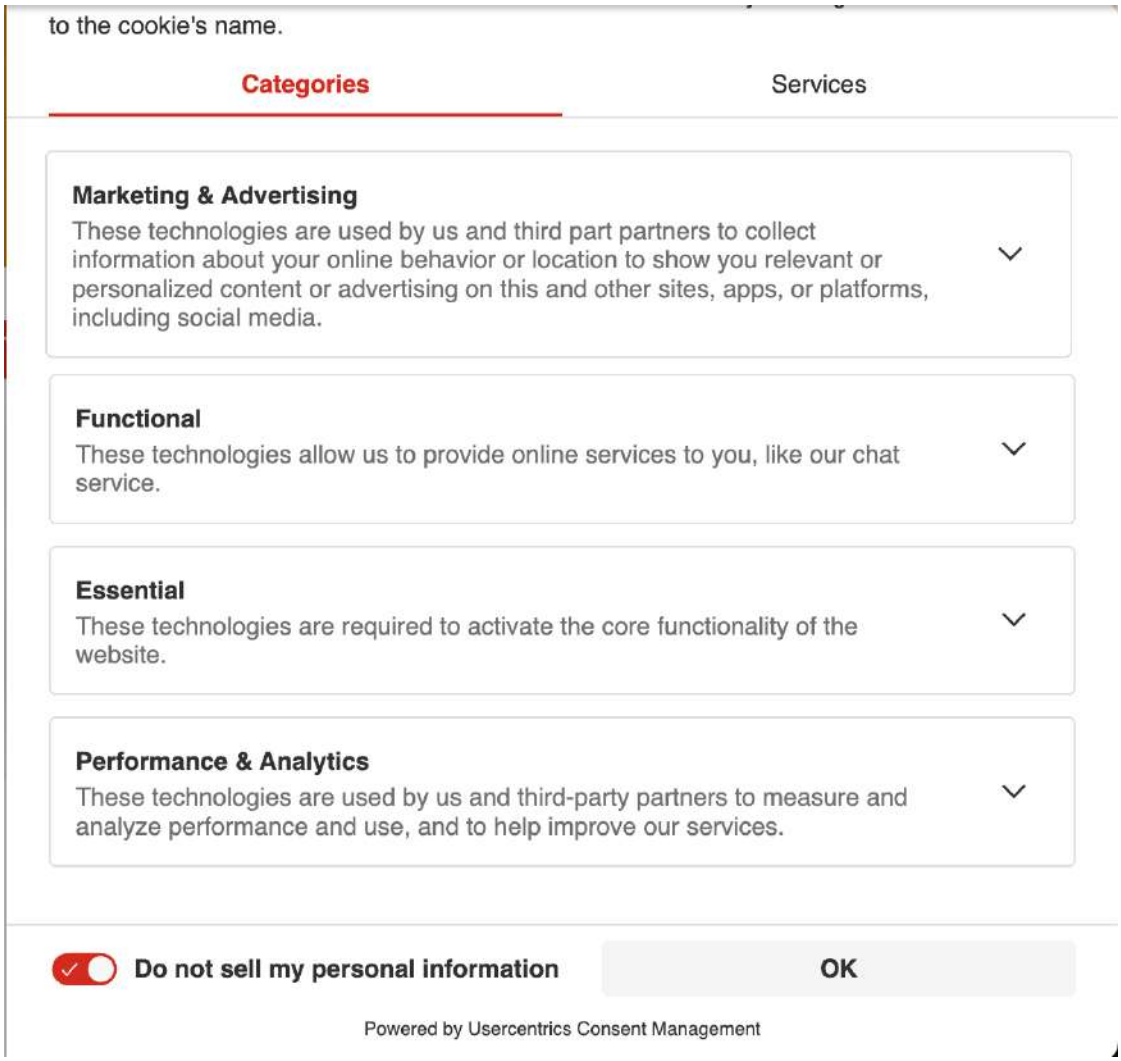
> **Information We Automatically Collect**
>
> Device and usage information and information collected via cookies and other tracking technologies: When you use Fender Properties, we collect some information that your technologies may automatically provide to us, including Internet or other electronic network activity information, such as your device's IP address, referring website, what pages your device visited, and the time that your device visited the Fender Properties. This may also include which browser and operating system you use, command link information, diagnostic information related to the Fender Properties, your mobile carrier, the device you use, and search terms…
>
> **TARGETED ADVERTISING AND ANALYTICS**
>
> We engage others to provide analytics services, serve advertisements, and perform related services across the web and in mobile apps. These entities may use cookies, web beacons, SDKs, device identifiers and other technologies to collect information about your use of the Services and other websites and applications, including your IP address and other identifiers, web browser and mobile network information, pages viewed, time spent on pages or in apps, links clicked, and conversion information. This information is used to deliver advertising targeted to your interests on other companies' sites or mobile apps and to analyze and track data including to understand how our ads perform and determine the popularity of certain content, and better understand your online activity…
>
> Our advertising partners then use that unique identifier to show ads that are more relevant to you across the web and in mobile apps. Some of the activities described in this section may constitute "targeted advertising," "sharing," or "selling" under certain state privacy laws…

30. Defendant further the categories of third-party cookies it used on the Website as follows in its "Manage Your Privacy Settings" window, which as accessible via the "More Information" link on the popup cookie consent banner:

[1] Fender Privacy Policy (Effective Date 6/1/2025) (available at https://www.fender.com/pages/privacy-policy) (the "Privacy Policy").



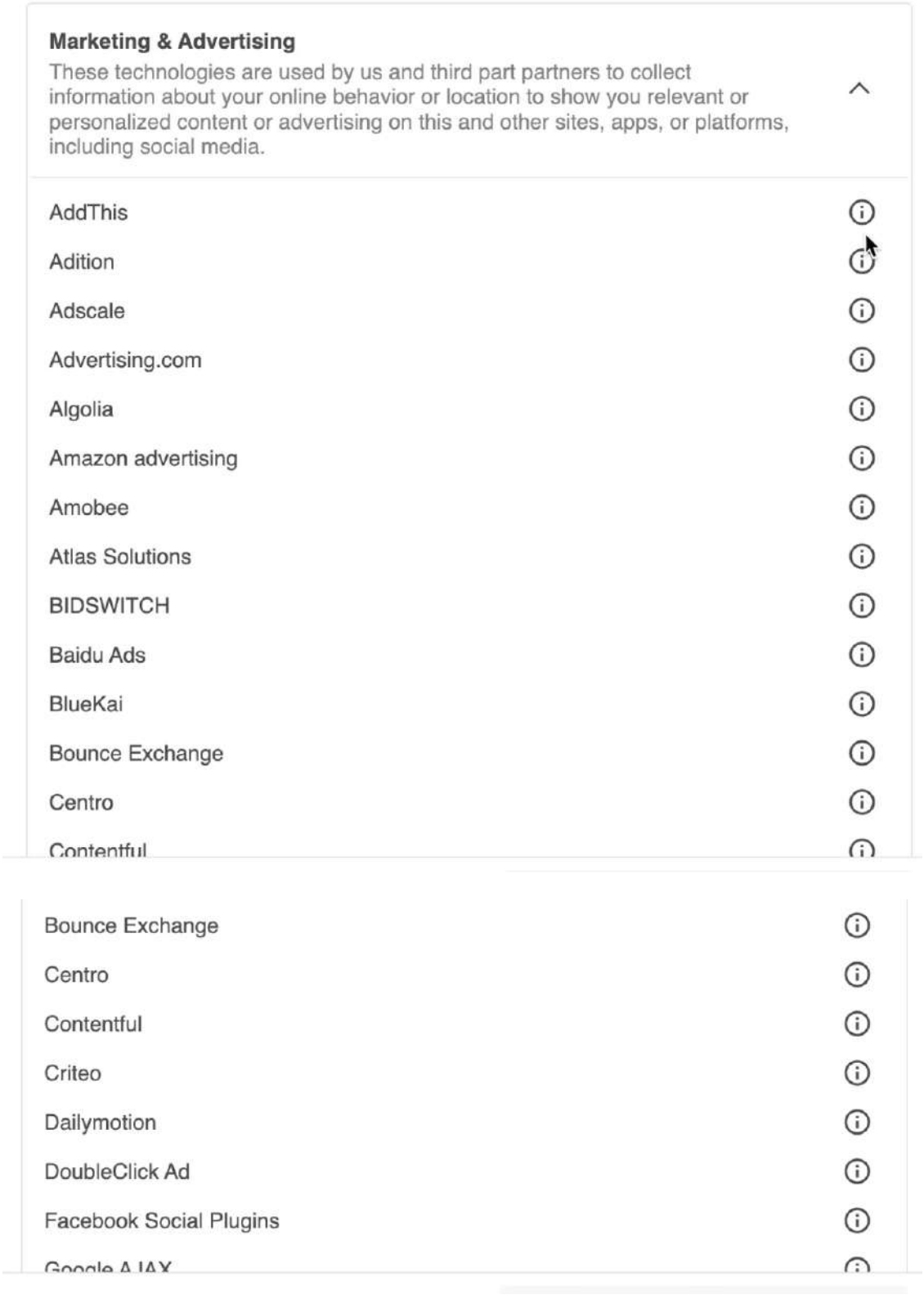
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

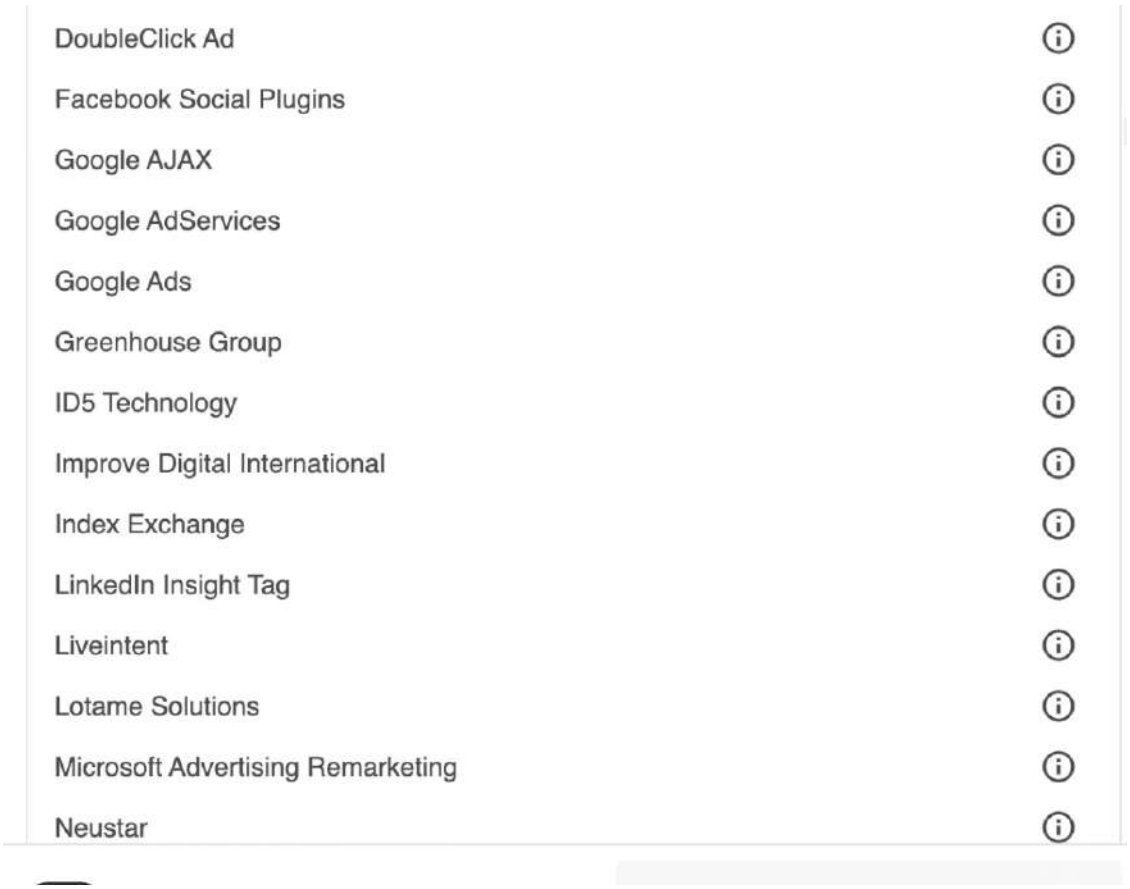


31. Defendant also identified some of providers of each category of the third-party cookies it used on the Website as follows in its "Manage Your Privacy Settings" window, which was accessible by expanding each category.

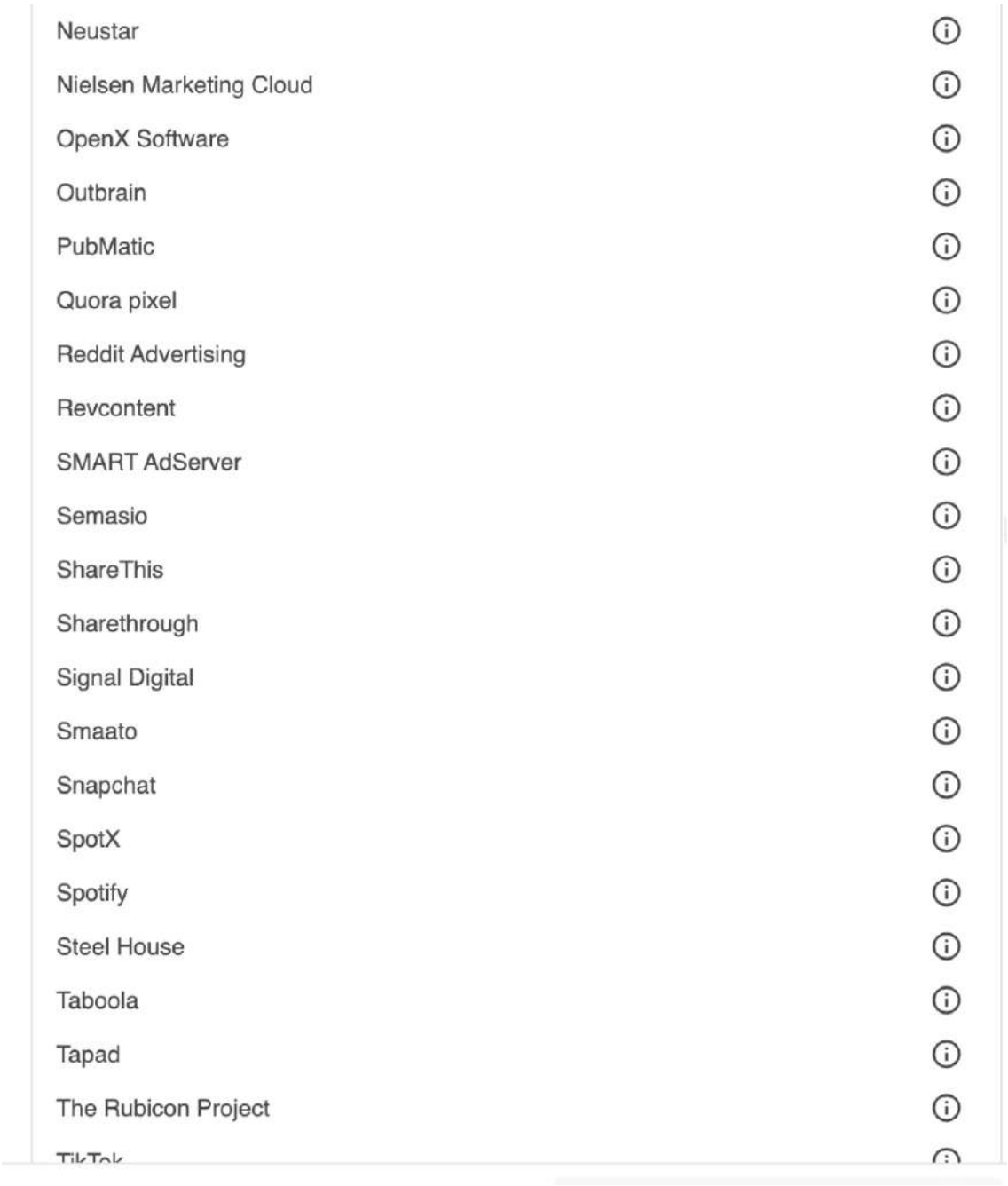
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

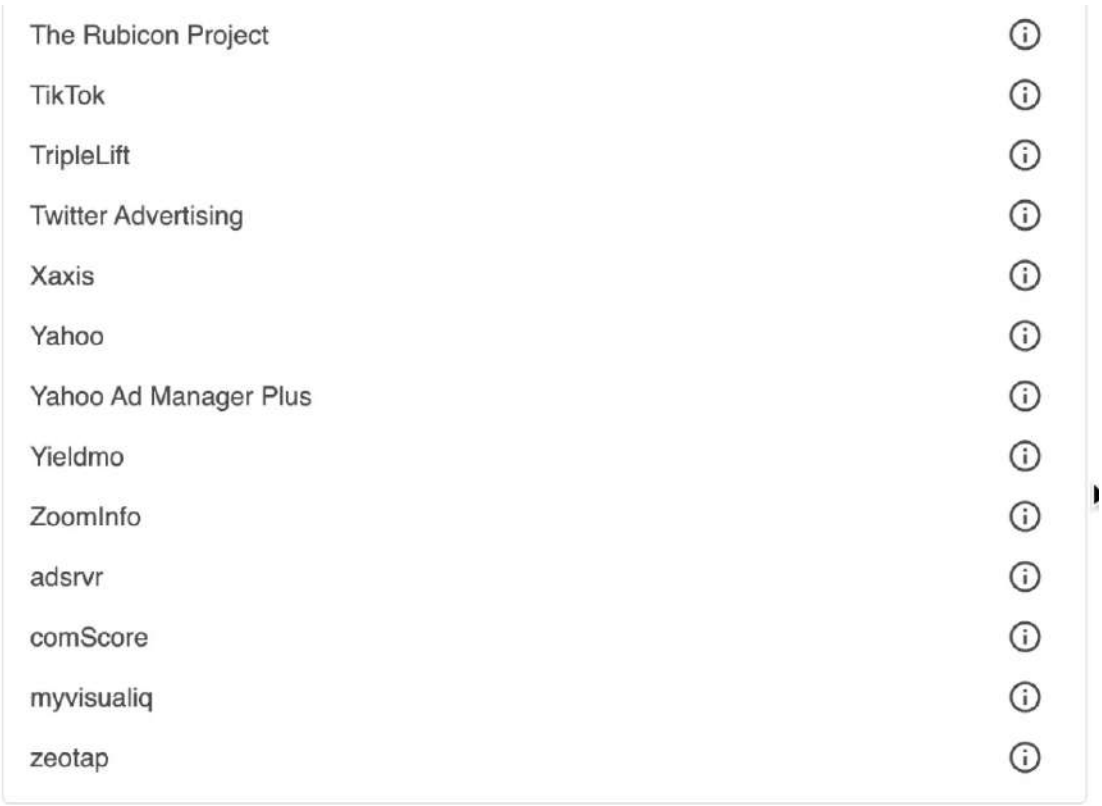
Marketing & Advertising





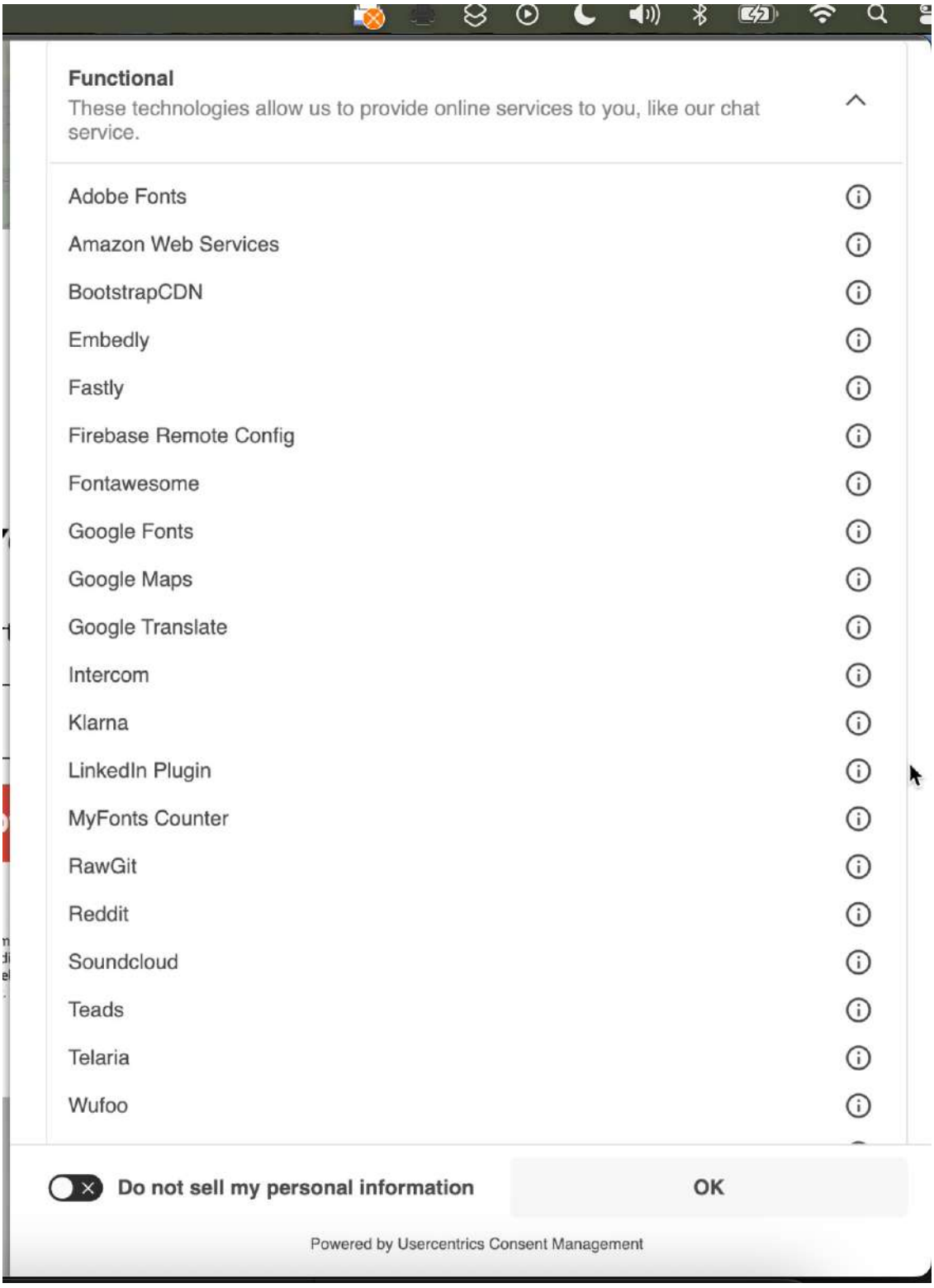
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

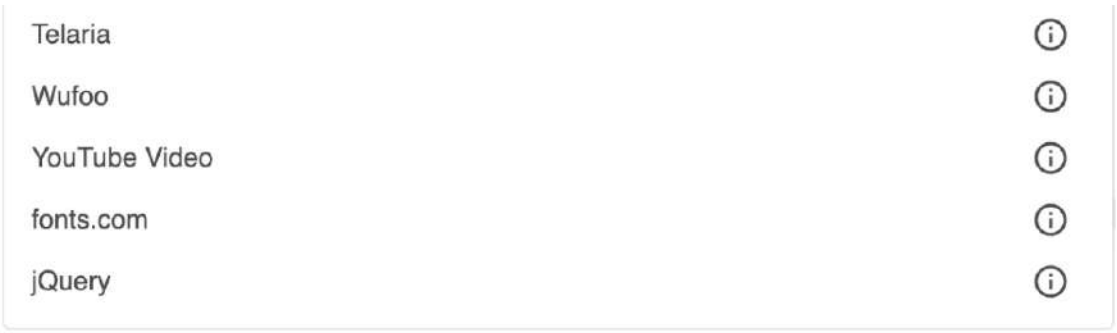

Neustar
Nielsen Marketing Cloud
OpenX Software
Outbrain
PubMatic
Quora pixel
Reddit Advertising
Revcontent
SMART AdServer
Semasio
ShareThis
Sharethrough
Signal Digital
Smaato
Snapchat
SpotX
Spotify
Steel House
Taboola
Tapad
The Rubicon Project
TikTok



[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

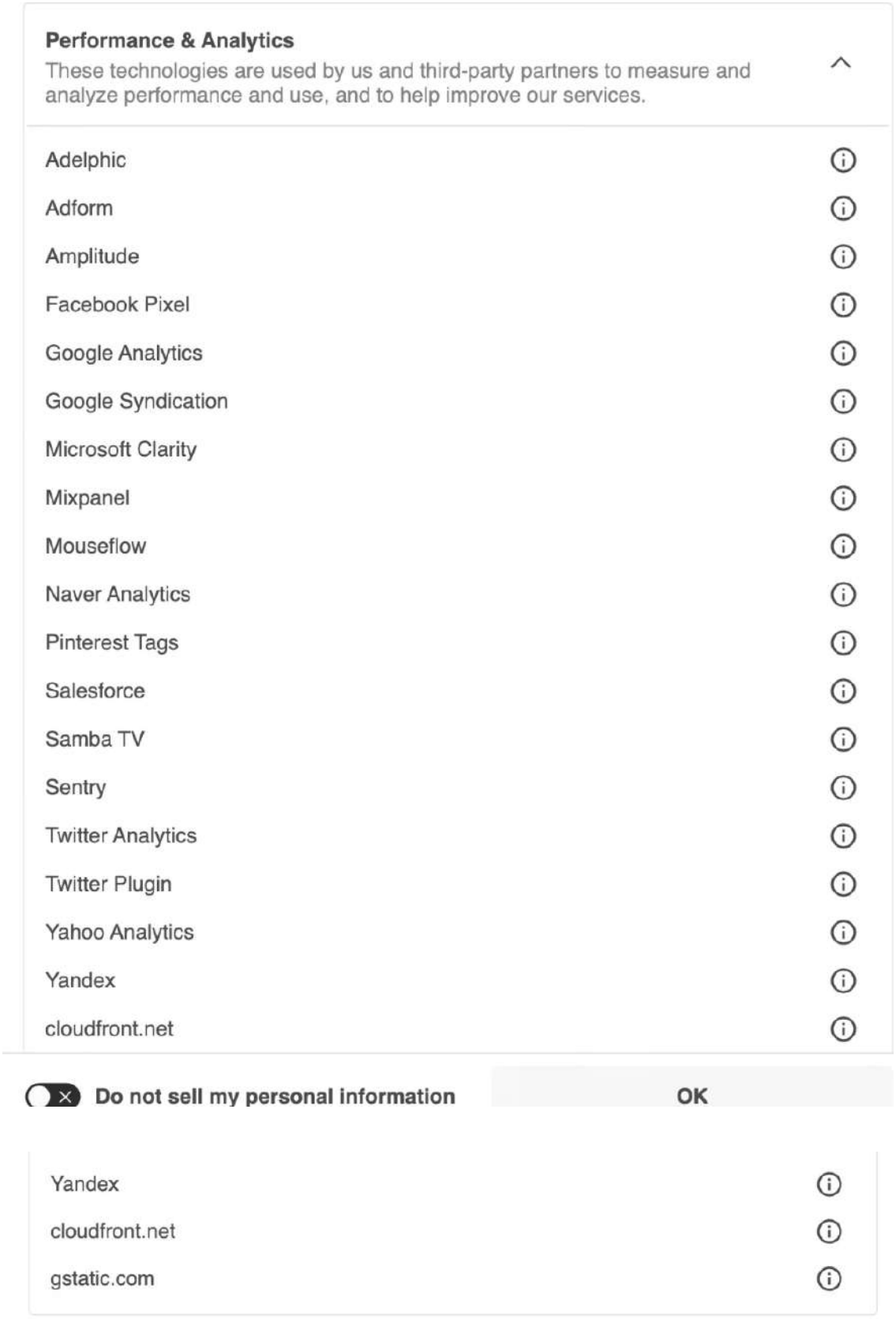
Functional


Functional
These technologies allow us to provide online services to you, like our chat service.
Adobe Fonts
Amazon Web Services
BootstrapCDN
Embedly
Fastly
Firebase Remote Config
Fontawesome
Google Fonts
Google Maps
Google Translate
Intercom
Klarna
LinkedIn Plugin
MyFonts Counter
RawGit
Reddit
Soundcloud
Teads
Telaria
Wufoo
Do not sell my personal information
OK
Powered by Usercentrics Consent Management



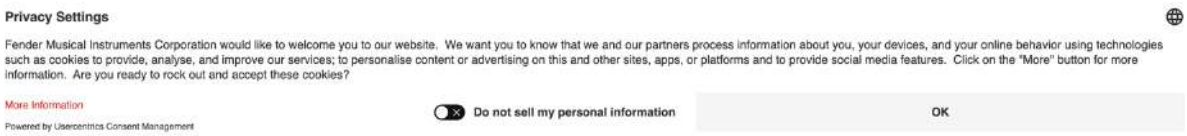
[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Performance & Analytics

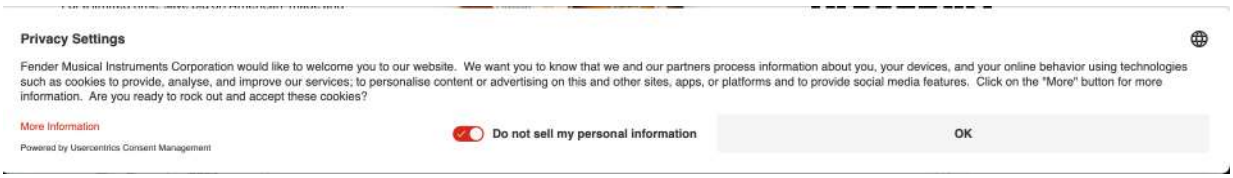


B. Defendant Falsely Informed Users That They Could Decline or Reject the Website's Use of Cookies.

32. When Plaintiffs and other consumers in California visited the Website, the Website immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the popup cookie consent banner, titled "Privacy Settings[,]" stated, "Fender Musical Instruments Corporation would like to welcome you to our website. We want you to know that we and our partners process information about you, your devices, and your online behavior using technologies such as cookies to provide, analyse, and improve our services; to personalise content or advertising on this and other sites, apps, or platforms and to provide social media features…Are you ready to rock out and accept these cookies?" Beneath this statement, Defendant presented users with the option to either select a button labelled "OK" or a toggle switch labeled "Do not sell my personal information[.]" The statements and options presented to users were as shown in the following screenshot from the Website:



33. Plaintiffs and other Website users who adjusted the "Do not sell my personal information" toggle switch, thereby indicating their choice and/or agreement to decline or reject cookies and tracking technologies in use on the Website, including those used for personalized advertising, analytics, and social media, as well as the sale or sharing of their personal information, could then continue to browse the Website (after also clicking the "OK" button), as the popup cookie consent banner disappeared. Below is a screenshot of the after the "Do not sell my personal information" toggle switch has been adjusted:



34. Defendant's popup cookie consent banner led Plaintiffs, and all those Website users similarly situated, to believe that they declined or rejected cookies and tracking

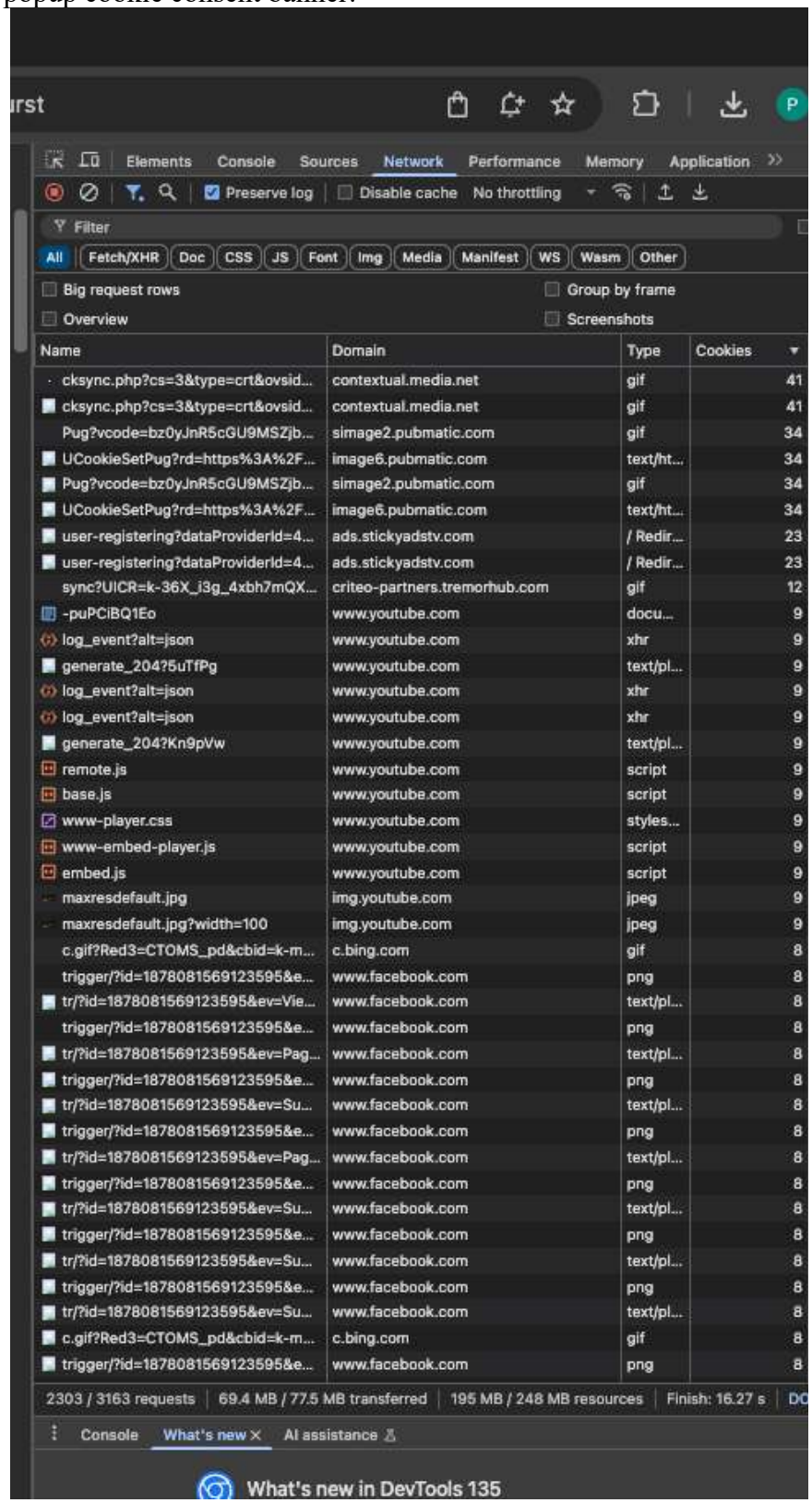
technologies, specifically including those cookies and tracking technologies used for personalized advertising, analytics, and social media, as well as all those cookies associated with the sale or sharing of their personal information. The banner further reasonably led Plaintiffs and those Website users similarly situated to believe that Defendant would not allow third parties, through cookies, to access their Private Communications with the Website, nor sell their personal data, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, upon adjusting the "Do not sell my personal information" toggle switch.

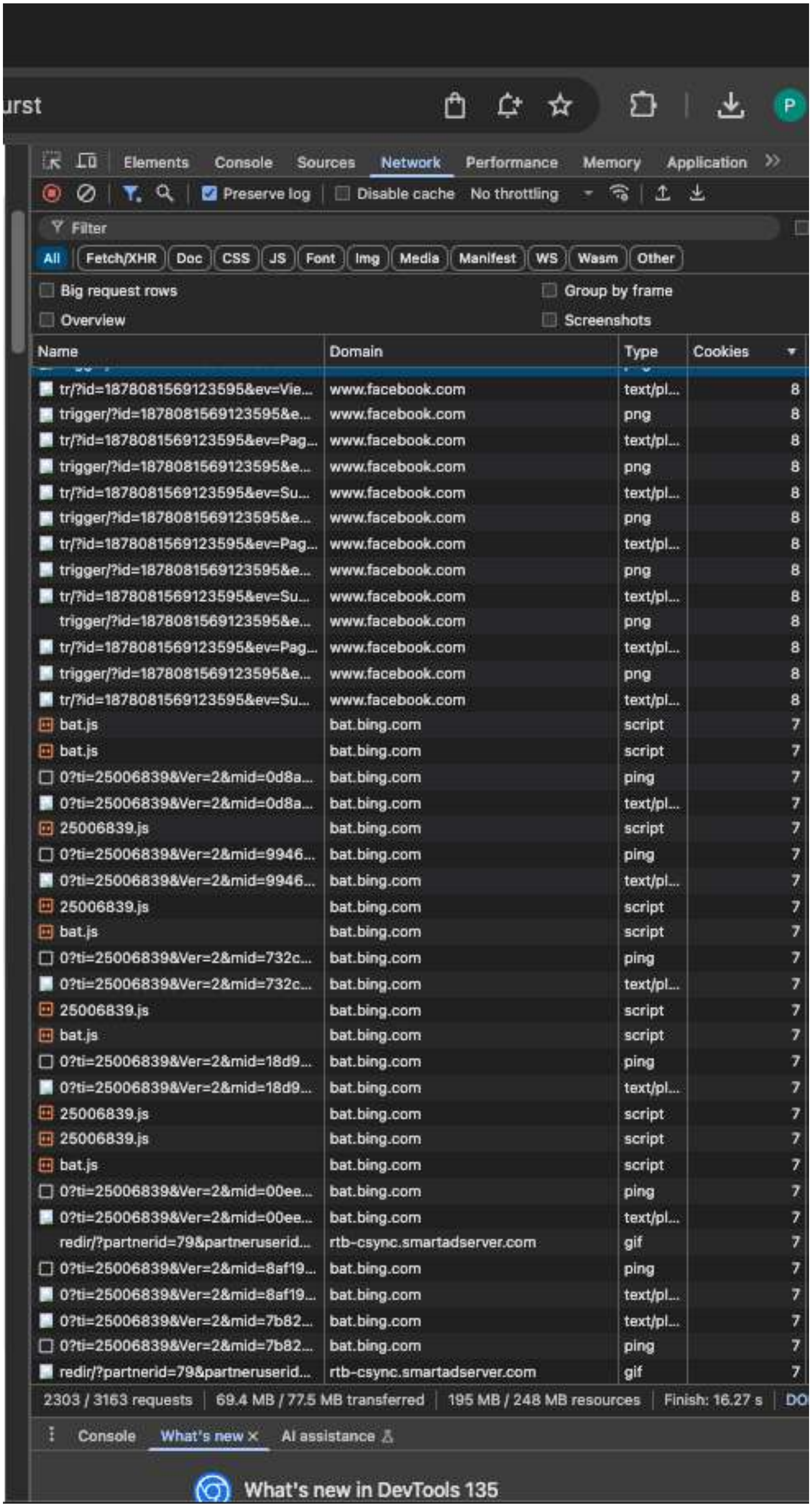
35. Defendant's representations, however, were false. In truth, Defendant did not abide by Plaintiffs' or other users' wishes. When Plaintiffs and other Website users adjusted the "Do not sell my personal information" toggle switch, they provided notice to Defendant that they did not consent to the placement or transmission of third-party cookies that would allow those parties to obtain their Private Communications with the Website, nor sell their personal information.

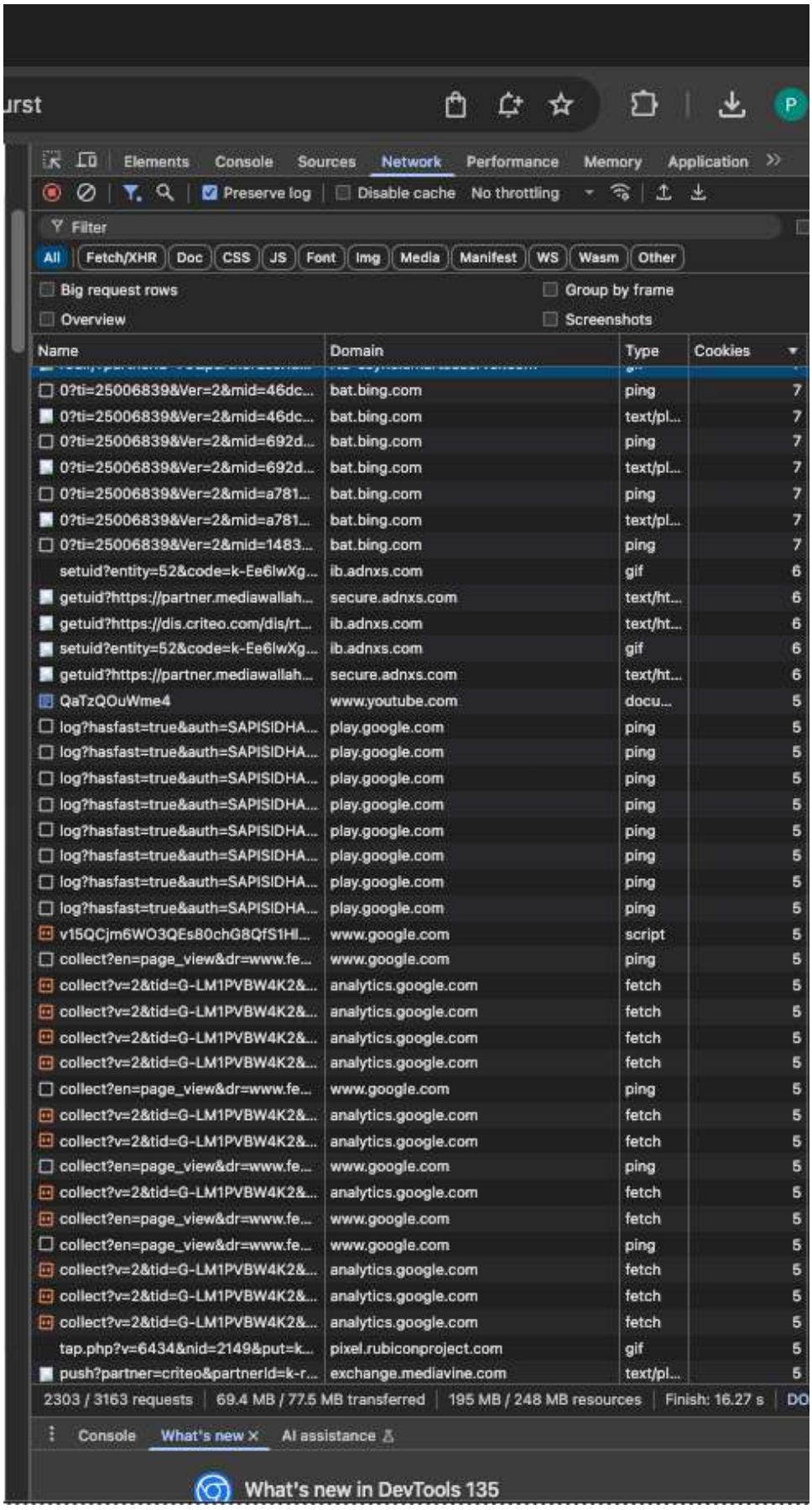
36. Nevertheless, even after receiving that notice, Defendant caused third-party tracking cookies, including the Third Parties' cookies, to be placed on Website users' browsers and devices and/or transmitted to the Third Parties which enabled the Third Parties to collect user data in real time that discloses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

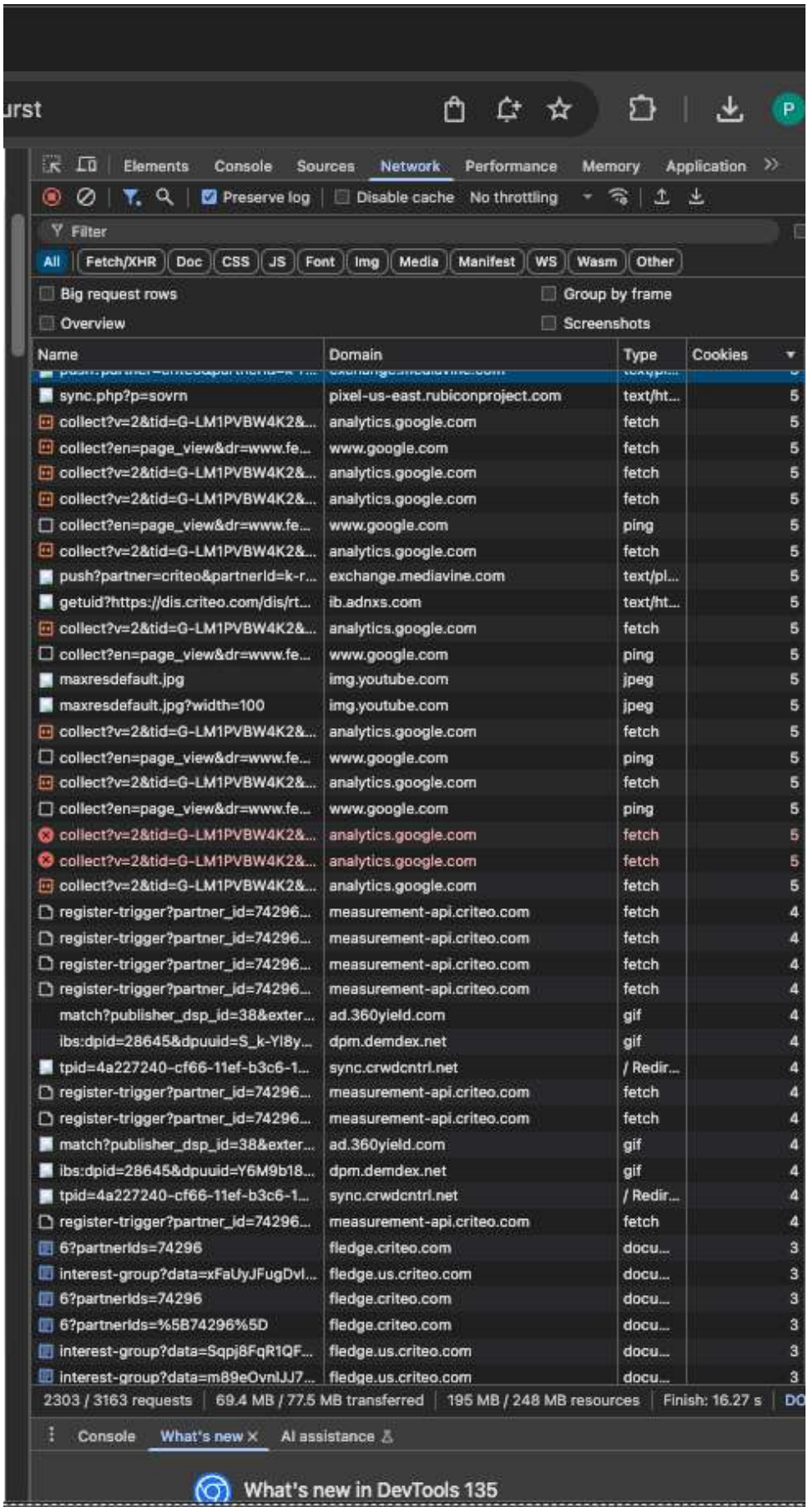
37. Some aspects of the operations of the Third Parties' cookies on the Website can be observed using specialized tools that log incoming and outgoing Website network transmissions. The following screenshot, obtained using one such tool, shows examples of the

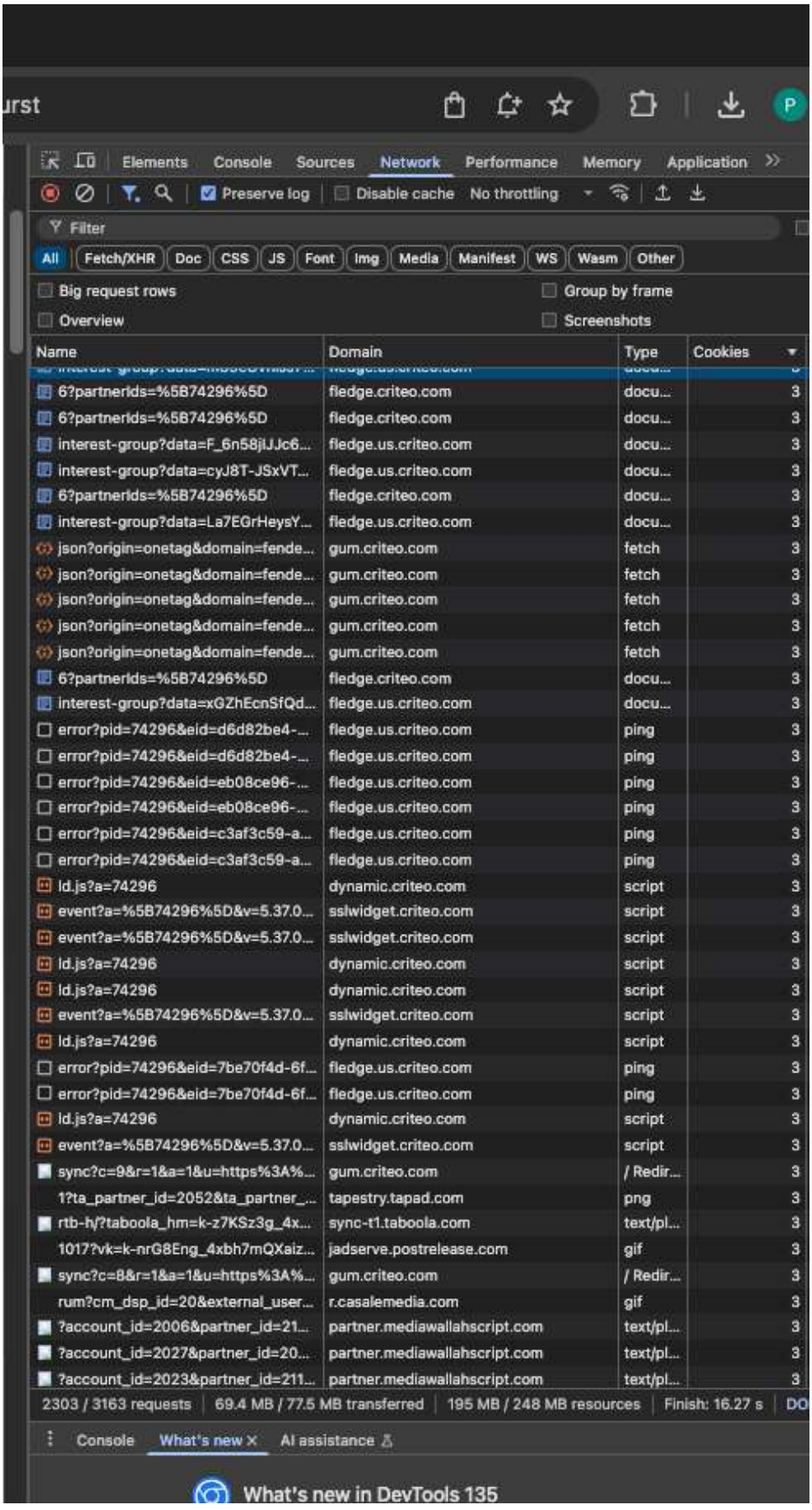
Third Parties' cookies being transmitted from a Website user's device and browser to the Third Parties, even after the user adjusted the "Do not sell my personal information" toggle switch on the Website's popup cookie consent banner:

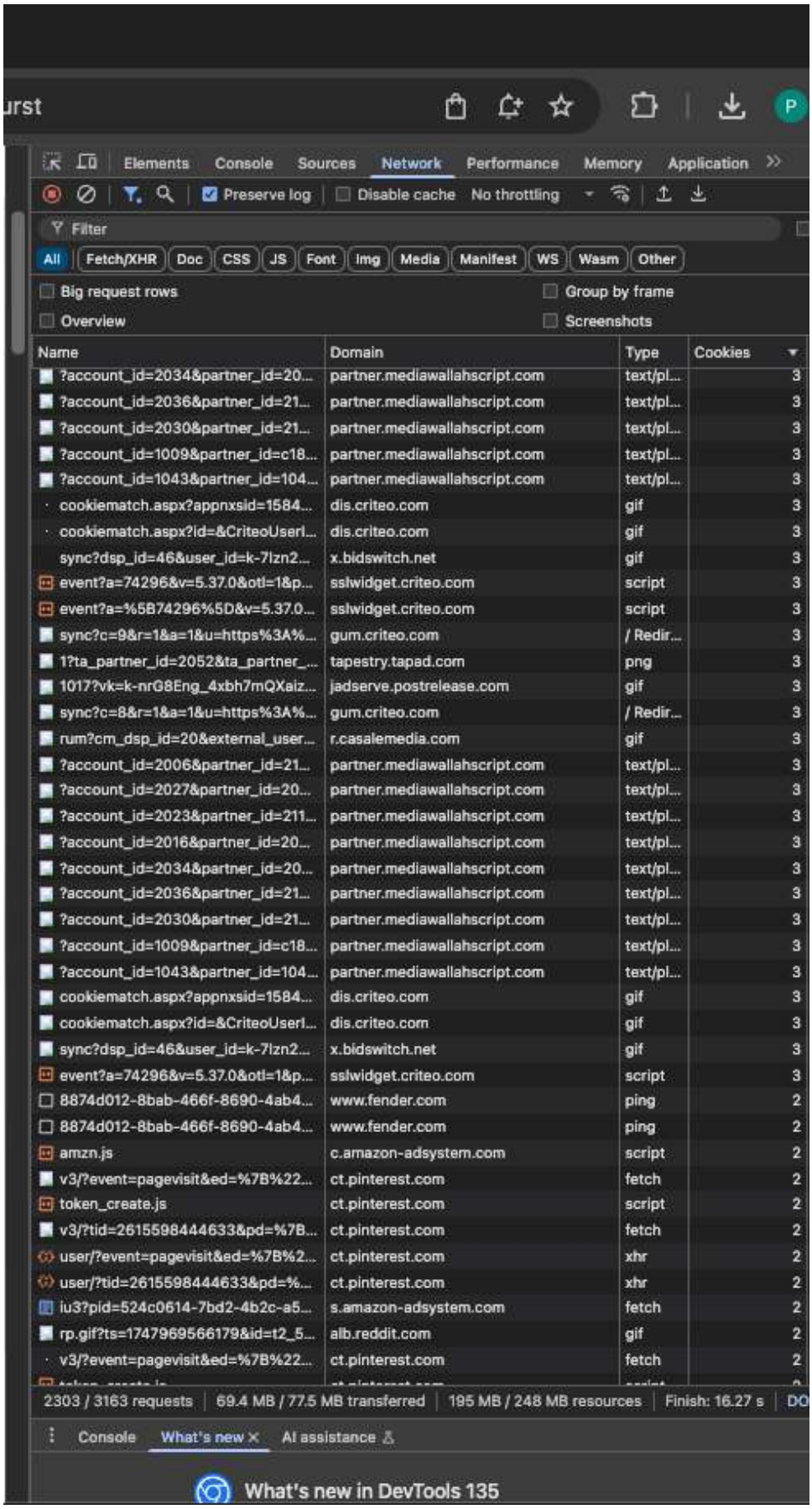


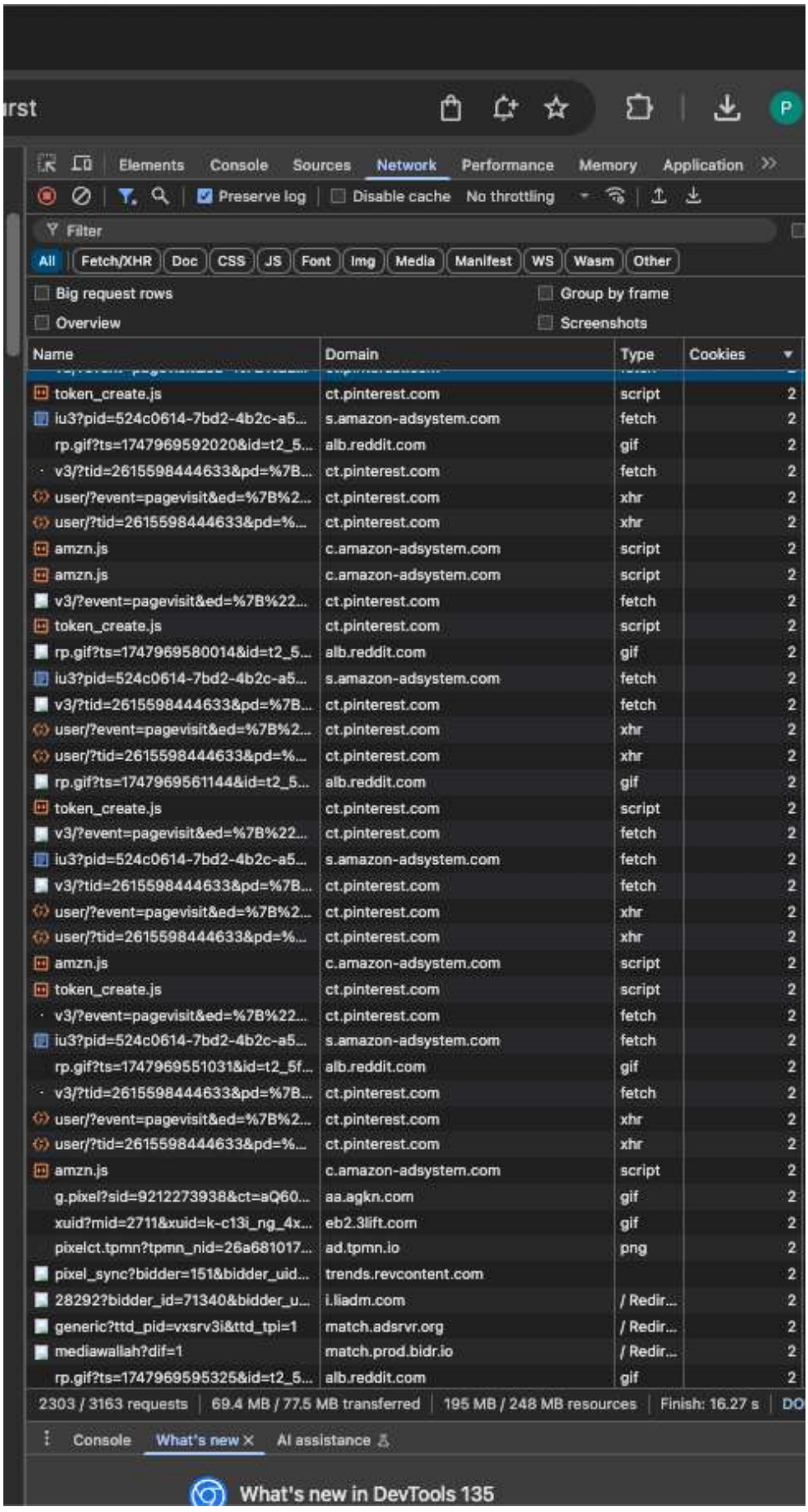

Elements Console Sources Network Performance Memory Application
Preserve log Disable cache No throttling
Filter
All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other
Big request rows Group by frame
Overview Screenshots
Name Domain Type Cookies
tr/?id=1878081569123595&ev=Vie... www.facebook.com text/pl... 8
trigger/?id=1878081569123595&e... www.facebook.com png 8
tr/?id=1878081569123595&ev=Pag... www.facebook.com text/pl... 8
trigger/?id=1878081569123595&e... www.facebook.com png 8
tr/?id=1878081569123595&ev=Su... www.facebook.com text/pl... 8
trigger/?id=1878081569123595&e... www.facebook.com png 8
tr/?id=1878081569123595&ev=Pag... www.facebook.com text/pl... 8
trigger/?id=1878081569123595&e... www.facebook.com png 8
tr/?id=1878081569123595&ev=Su... www.facebook.com text/pl... 8
trigger/?id=1878081569123595&e... www.facebook.com png 8
tr/?id=1878081569123595&ev=Pag... www.facebook.com text/pl... 8
trigger/?id=1878081569123595&e... www.facebook.com png 8
tr/?id=1878081569123595&ev=Su... www.facebook.com text/pl... 8
bat.js bat.bing.com script 7
bat.js bat.bing.com script 7
0?ti=25006839&Ver=2&mid=0d8a... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=0d8a... bat.bing.com text/pl... 7
25006839.js bat.bing.com script 7
0?ti=25006839&Ver=2&mid=9946... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=9946... bat.bing.com text/pl... 7
25006839.js bat.bing.com script 7
bat.js bat.bing.com script 7
0?ti=25006839&Ver=2&mid=732c... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=732c... bat.bing.com text/pl... 7
25006839.js bat.bing.com script 7
bat.js bat.bing.com script 7
0?ti=25006839&Ver=2&mid=18d9... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=18d9... bat.bing.com text/pl... 7
25006839.js bat.bing.com script 7
25006839.js bat.bing.com script 7
bat.js bat.bing.com script 7
0?ti=25006839&Ver=2&mid=00ee... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=00ee... bat.bing.com text/pl... 7
redir/?partnerid=79&partneruserid... rtb-csync.smartadserver.com gif 7
0?ti=25006839&Ver=2&mid=8af19... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=8af19... bat.bing.com text/pl... 7
0?ti=25006839&Ver=2&mid=7b82... bat.bing.com text/pl... 7
0?ti=25006839&Ver=2&mid=7b82... bat.bing.com ping 7
redir/?partnerid=79&partneruserid... rtb-csync.smartadserver.com gif 7
2303 / 3163 requests 69.4 MB / 77.5 MB transferred 195 MB / 248 MB resources Finish: 16.27 s
Console What's new AI assistance
What's new in DevTools 135

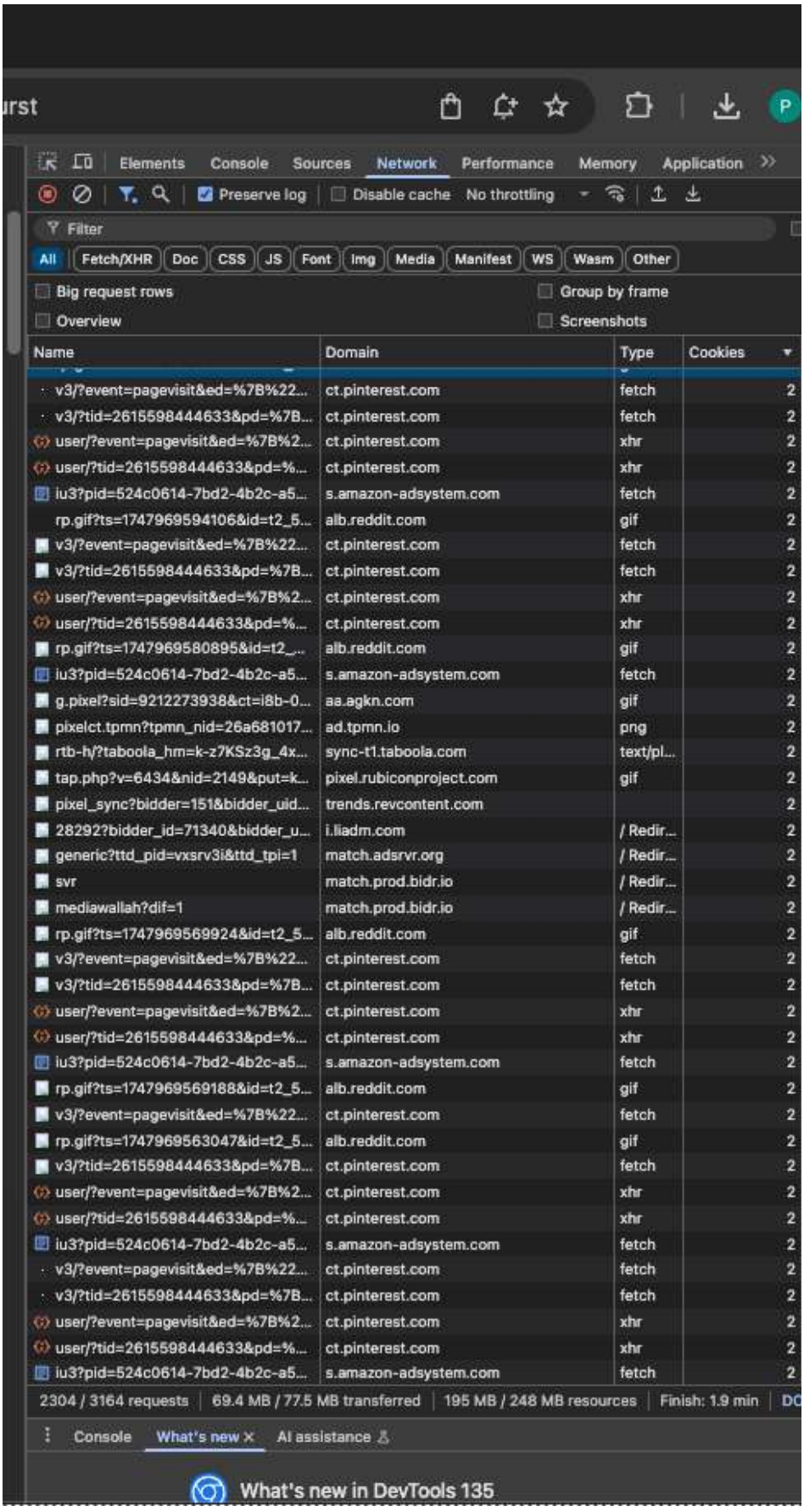

Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
Name
Domain
Type
Cookies
0?ti=25006839&Ver=2&mid=46dc... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=46dc... bat.bing.com text/pl... 7
0?ti=25006839&Ver=2&mid=692d... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=692d... bat.bing.com text/pl... 7
0?ti=25006839&Ver=2&mid=a781... bat.bing.com ping 7
0?ti=25006839&Ver=2&mid=a781... bat.bing.com text/pl... 7
0?ti=25006839&Ver=2&mid=1483... bat.bing.com ping 7
setuid?entity=52&code=k-Ee6lwXg... ib.adnxs.com gif 6
getuid?https://partner.mediawallah... secure.adnxs.com text/ht... 6
getuid?https://dis.criteo.com/dis/rt... ib.adnxs.com text/ht... 6
setuid?entity=52&code=k-Ee6lwXg... ib.adnxs.com gif 6
getuid?https://partner.mediawallah... secure.adnxs.com text/ht... 6
QaTzQOuWme4 www.youtube.com docu... 5
log?hasfast=true&auth=SAPISIDHA... play.google.com ping 5
log?hasfast=true&auth=SAPISIDHA... play.google.com ping 5
log?hasfast=true&auth=SAPISIDHA... play.google.com ping 5
log?hasfast=true&auth=SAPISIDHA... play.google.com ping 5
log?hasfast=true&auth=SAPISIDHA... play.google.com ping 5
log?hasfast=true&auth=SAPISIDHA... play.google.com ping 5
log?hasfast=true&auth=SAPISIDHA... play.google.com ping 5
log?hasfast=true&auth=SAPISIDHA... play.google.com ping 5
v15QCjm6WO3QEs80chG8QfS1HI... www.google.com script 5
collect?en=page_view&dr=www.fe... www.google.com ping 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com ping 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com ping 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com ping 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
tap.php?v=6434&nid=2149&put=k... pixel.rubiconproject.com gif 5
push?partner=criteo&partnerId=k-r... exchange.mediavine.com text/pl... 5
2303 / 3163 requests
69.4 MB / 77.5 MB transferred
195 MB / 248 MB resources
Finish: 16.27 s
Console
What's new
AI assistance
What's new in DevTools 135


Elements Console Sources Network Performance Memory Application
Preserve log Disable cache No throttling
Filter
All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other
Big request rows
Group by frame
Overview
Screenshots
Name Domain Type Cookies
sync.php?p=sovrn pixel-us-east.rubiconproject.com text/ht... 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com ping 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
push?partner=criteo&partnerId=k-r... exchange.mediavine.com text/pl... 5
getuid?https://dis.criteo.com/dis/rt... ib.adnxs.com text/ht... 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com ping 5
maxresdefault.jpg img.youtube.com jpeg 5
maxresdefault.jpg?width=100 img.youtube.com jpeg 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com ping 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?en=page_view&dr=www.fe... www.google.com ping 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
collect?v=2&tid=G-LM1PVBW4K2&... analytics.google.com fetch 5
register-trigger?partner_id=74296... measurement-api.criteo.com fetch 4
register-trigger?partner_id=74296... measurement-api.criteo.com fetch 4
register-trigger?partner_id=74296... measurement-api.criteo.com fetch 4
register-trigger?partner_id=74296... measurement-api.criteo.com fetch 4
match?publisher_dsp_id=38&exter... ad.360yield.com gif 4
ibs:dpid=28645&dpuuid=S_k-Yl8y... dpm.demdex.net gif 4
tpid=4a227240-cf66-11ef-b3c6-1... sync.crwdcntrl.net / Redir... 4
register-trigger?partner_id=74296... measurement-api.criteo.com fetch 4
register-trigger?partner_id=74296... measurement-api.criteo.com fetch 4
match?publisher_dsp_id=38&exter... ad.360yield.com gif 4
ibs:dpid=28645&dpuuid=Y6M9b18... dpm.demdex.net gif 4
tpid=4a227240-cf66-11ef-b3c6-1... sync.crwdcntrl.net / Redir... 4
register-trigger?partner_id=74296... measurement-api.criteo.com fetch 4
6?partnerIds=74296 fledge.criteo.com docu... 3
interest-group?data=xFaUyJFugDvl... fledge.us.criteo.com docu... 3
6?partnerIds=74296 fledge.criteo.com docu... 3
6?partnerIds=%5B74296%5D fledge.criteo.com docu... 3
interest-group?data=Sqpj8FqR1QF... fledge.us.criteo.com docu... 3
interest-group?data=m89eOvnlJJ7... fledge.us.criteo.com docu... 3
2303 / 3163 requests 69.4 MB / 77.5 MB transferred 195 MB / 248 MB resources Finish: 16.27 s
Console What's new AI assistance
What's new in DevTools 135

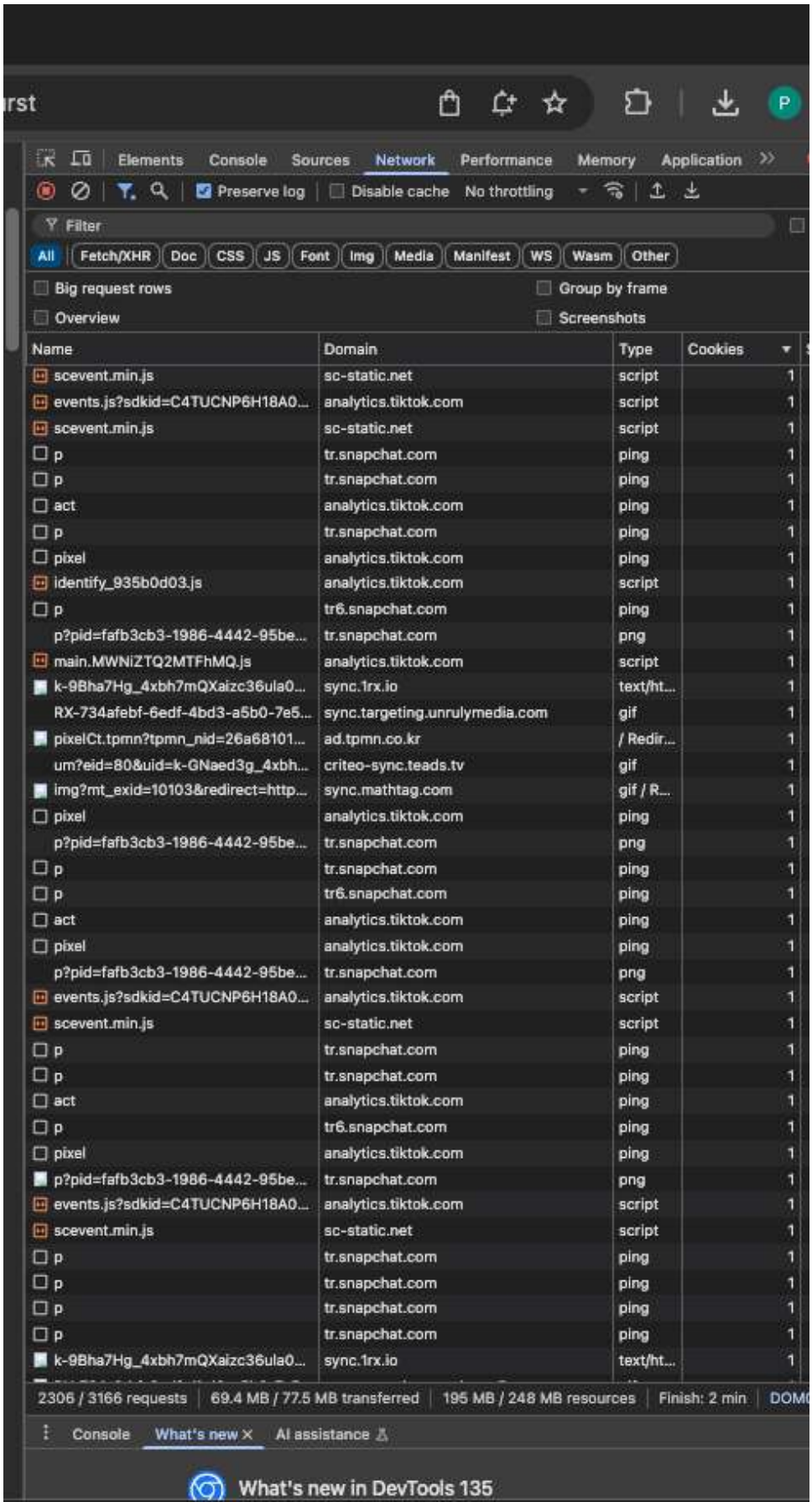

Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
Name
Domain
Type
Cookies
6?partnerIds=%5B74296%5D fledge.criteo.com docu... 3
6?partnerIds=%5B74296%5D fledge.criteo.com docu... 3
interest-group?data=F_6n58jIJJc6... fledge.us.criteo.com docu... 3
interest-group?data=cyJ8T-JSxVT... fledge.us.criteo.com docu... 3
6?partnerIds=%5B74296%5D fledge.criteo.com docu... 3
interest-group?data=La7EGrHeysY... fledge.us.criteo.com docu... 3
json?origin=onetag&domain=fende... gum.criteo.com fetch 3
json?origin=onetag&domain=fende... gum.criteo.com fetch 3
json?origin=onetag&domain=fende... gum.criteo.com fetch 3
json?origin=onetag&domain=fende... gum.criteo.com fetch 3
json?origin=onetag&domain=fende... gum.criteo.com fetch 3
6?partnerIds=%5B74296%5D fledge.criteo.com docu... 3
interest-group?data=xGZhEcnSfQd... fledge.us.criteo.com docu... 3
error?pid=74296&eid=d6d82be4-... fledge.us.criteo.com ping 3
error?pid=74296&eid=d6d82be4-... fledge.us.criteo.com ping 3
error?pid=74296&eid=eb08ce96-... fledge.us.criteo.com ping 3
error?pid=74296&eid=eb08ce96-... fledge.us.criteo.com ping 3
error?pid=74296&eid=c3af3c59-a... fledge.us.criteo.com ping 3
error?pid=74296&eid=c3af3c59-a... fledge.us.criteo.com ping 3
ld.js?a=74296 dynamic.criteo.com script 3
event?a=%5B74296%5D&v=5.37.0... sslwidget.criteo.com script 3
event?a=%5B74296%5D&v=5.37.0... sslwidget.criteo.com script 3
ld.js?a=74296 dynamic.criteo.com script 3
ld.js?a=74296 dynamic.criteo.com script 3
event?a=%5B74296%5D&v=5.37.0... sslwidget.criteo.com script 3
ld.js?a=74296 dynamic.criteo.com script 3
error?pid=74296&eid=7be70f4d-6f... fledge.us.criteo.com ping 3
error?pid=74296&eid=7be70f4d-6f... fledge.us.criteo.com ping 3
ld.js?a=74296 dynamic.criteo.com script 3
event?a=%5B74296%5D&v=5.37.0... sslwidget.criteo.com script 3
sync?c=9&r=1&a=1&u=https%3A%... gum.criteo.com / Redir... 3
1?ta_partner_id=2052&ta_partner_... tapestry.tapad.com png 3
rtb-h/?taboola_hm=k-z7KSz3g_4x... sync-t1.taboola.com text/pl... 3
1017?vk=k-nrG8Eng_4xbh7mQXaiz... jadserve.postrelease.com gif 3
sync?c=8&r=1&a=1&u=https%3A%... gum.criteo.com / Redir... 3
rum?cm_dsp_id=20&external_user... r.casalemedia.com gif 3
?account_id=2006&partner_id=21... partner.mediawallahscript.com text/pl... 3
?account_id=2027&partner_id=20... partner.mediawallahscript.com text/pl... 3
?account_id=2023&partner_id=211... partner.mediawallahscript.com text/pl... 3
2303 / 3163 requests
69.4 MB / 77.5 MB transferred
195 MB / 248 MB resources
Finish: 16.27 s
Console
What's new
AI assistance
What's new in DevTools 135

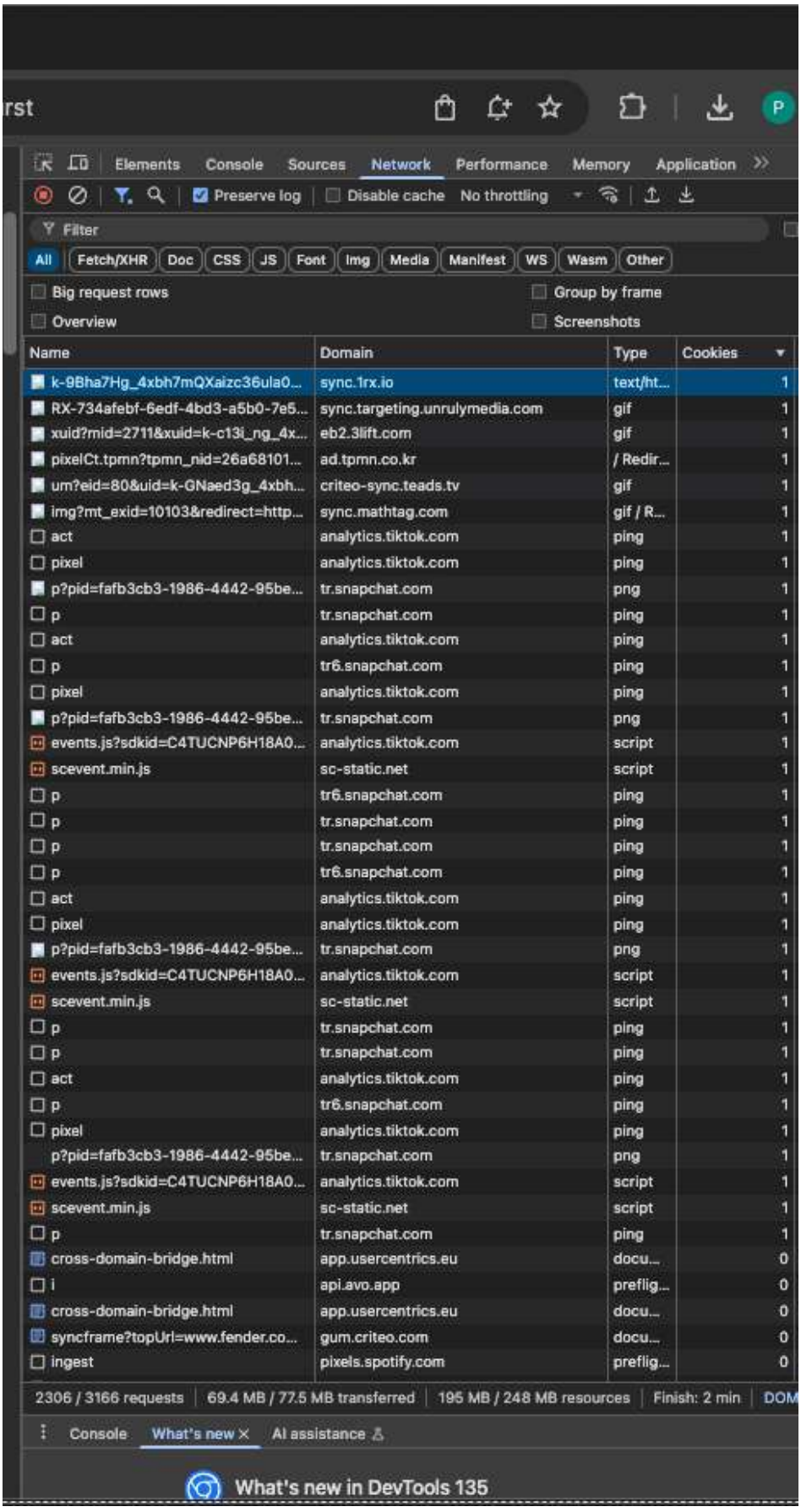

Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
Name
Domain
Type
Cookies
2303 / 3163 requests
69.4 MB / 77.5 MB transferred
195 MB / 248 MB resources
Finish: 16.27 s
Console
What's new
AI assistance
What's new in DevTools 135


Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
Name
Domain
Type
Cookies
token_create.js ct.pinterest.com script 2
iu3?pid=524c0614-7bd2-4b2c-a5... s.amazon-adsystem.com fetch 2
rp.gif?ts=1747969592020&id=t2_5... alb.reddit.com gif 2
v3/?tid=2615598444633&pd=%7B... ct.pinterest.com fetch 2
user/?event=pagevisit&ed=%7B%2... ct.pinterest.com xhr 2
user/?tid=2615598444633&pd=%... ct.pinterest.com xhr 2
amzn.js c.amazon-adsystem.com script 2
amzn.js c.amazon-adsystem.com script 2
v3/?event=pagevisit&ed=%7B%22... ct.pinterest.com fetch 2
token_create.js ct.pinterest.com script 2
rp.gif?ts=1747969580014&id=t2_5... alb.reddit.com gif 2
iu3?pid=524c0614-7bd2-4b2c-a5... s.amazon-adsystem.com fetch 2
v3/?tid=2615598444633&pd=%7B... ct.pinterest.com fetch 2
user/?event=pagevisit&ed=%7B%2... ct.pinterest.com xhr 2
user/?tid=2615598444633&pd=%... ct.pinterest.com xhr 2
rp.gif?ts=1747969561144&id=t2_5... alb.reddit.com gif 2
token_create.js ct.pinterest.com script 2
v3/?event=pagevisit&ed=%7B%22... ct.pinterest.com fetch 2
iu3?pid=524c0614-7bd2-4b2c-a5... s.amazon-adsystem.com fetch 2
v3/?tid=2615598444633&pd=%7B... ct.pinterest.com fetch 2
user/?event=pagevisit&ed=%7B%2... ct.pinterest.com xhr 2
user/?tid=2615598444633&pd=%... ct.pinterest.com xhr 2
amzn.js c.amazon-adsystem.com script 2
token_create.js ct.pinterest.com script 2
v3/?event=pagevisit&ed=%7B%22... ct.pinterest.com fetch 2
iu3?pid=524c0614-7bd2-4b2c-a5... s.amazon-adsystem.com fetch 2
rp.gif?ts=1747969551031&id=t2_5f... alb.reddit.com gif 2
v3/?tid=2615598444633&pd=%7B... ct.pinterest.com fetch 2
user/?event=pagevisit&ed=%7B%2... ct.pinterest.com xhr 2
user/?tid=2615598444633&pd=%... ct.pinterest.com xhr 2
amzn.js c.amazon-adsystem.com script 2
g.pixel?sid=9212273938&ct=aQ60... aa.agkn.com gif 2
xuid?mid=2711&xuid=k-c13i_ng_4x... eb2.3lift.com gif 2
pixelct.tpmn?tpmn_nid=26a681017... ad.tpmn.io png 2
pixel_sync?bidder=151&bidder_uid... trends.revcontent.com 2
28292?bidder_id=71340&bidder_u... i.liadm.com / Redir... 2
generic?ttd_pid=vxsrv3i&ttd_tpi=1 match.adsrvr.org / Redir... 2
mediawallah?dif=1 match.prod.bidr.io / Redir... 2
rp.gif?ts=1747969595325&id=t2_5... alb.reddit.com gif 2
2303 / 3163 requests
69.4 MB / 77.5 MB transferred
195 MB / 248 MB resources
Finish: 16.27 s
Console
What's new
AI assistance
What's new in DevTools 135


Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
Name
Domain
Type
Cookies
2304 / 3164 requests
69.4 MB / 77.5 MB transferred
195 MB / 248 MB resources
Finish: 1.9 min
Console
What's new
AI assistance
What's new in DevTools 135


Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
Name
Domain
Type
Cookies
rp.gif?ts=1747969555782&id=t2_5... alb.reddit.com gif 2
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
scevent.min.js sc-static.net script 1
p tr.snapchat.com ping 1
act analytics.tiktok.com ping 1
p tr.snapchat.com ping 1
pixel analytics.tiktok.com ping 1
identify_935b0d03.js analytics.tiktok.com script 1
p tr6.snapchat.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
main.MWNiZTQ2MTFhMQ.js analytics.tiktok.com script 1
act analytics.tiktok.com ping 1
p tr.snapchat.com ping 1
pixel analytics.tiktok.com ping 1
identify_935b0d03.js analytics.tiktok.com script 1
p tr6.snapchat.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
main.MWNiZTQ2MTFhMQ.js analytics.tiktok.com script 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
scevent.min.js sc-static.net script 1
p tr.snapchat.com ping 1
act analytics.tiktok.com ping 1
p tr.snapchat.com ping 1
pixel analytics.tiktok.com ping 1
identify_935b0d03.js analytics.tiktok.com script 1
p tr6.snapchat.com ping 1
scevent.min.js sc-static.net script 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
main.MWNiZTQ2MTFhMQ.js analytics.tiktok.com script 1
p tr.snapchat.com ping 1
act analytics.tiktok.com ping 1
p tr.snapchat.com ping 1
pixel analytics.tiktok.com ping 1
identify_935b0d03.js analytics.tiktok.com script 1
p tr6.snapchat.com ping 1
main.MWNiZTQ2MTFhMQ.js analytics.tiktok.com script 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
2306 / 3166 requests
69.4 MB / 77.5 MB transferred
195 MB / 248 MB resources
Finish: 2 min
Console
What's new
AI assistance
What's new in DevTools 135


Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
Name
Domain
Type
Cookies
scevent.min.js sc-static.net script 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
scevent.min.js sc-static.net script 1
p tr.snapchat.com ping 1
p tr.snapchat.com ping 1
act analytics.tiktok.com ping 1
p tr.snapchat.com ping 1
pixel analytics.tiktok.com ping 1
identify_935b0d03.js analytics.tiktok.com script 1
p tr6.snapchat.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
main.MWNiZTQ2MTFhMQ.js analytics.tiktok.com script 1
k-9Bha7Hg_4xbh7mQXaizc36ula0... sync.1rx.io text/ht... 1
RX-734afebf-6edf-4bd3-a5b0-7e5... sync.targeting.unrulymedia.com gif 1
pixelCt.tpmn?tpmn_nid=26a68101... ad.tpmn.co.kr / Redir... 1
um?eid=80&uid=k-GNaed3g_4xbh... criteo-sync.teads.tv gif 1
img?mt_exid=10103&redirect=http... sync.mathtag.com gif / R... 1
pixel analytics.tiktok.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
p tr.snapchat.com ping 1
p tr6.snapchat.com ping 1
act analytics.tiktok.com ping 1
pixel analytics.tiktok.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
scevent.min.js sc-static.net script 1
p tr.snapchat.com ping 1
p tr.snapchat.com ping 1
act analytics.tiktok.com ping 1
p tr6.snapchat.com ping 1
pixel analytics.tiktok.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
scevent.min.js sc-static.net script 1
p tr.snapchat.com ping 1
p tr.snapchat.com ping 1
p tr.snapchat.com ping 1
p tr.snapchat.com ping 1
k-9Bha7Hg_4xbh7mQXaizc36ula0... sync.1rx.io text/ht... 1
2306 / 3166 requests
69.4 MB / 77.5 MB transferred
195 MB / 248 MB resources
Finish: 2 min
Console
What's new
AI assistance
What's new in DevTools 135


rst
Elements
Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Big request rows
Group by frame
Overview
Screenshots
Name
Domain
Type
Cookies
k-9Bha7Hg_4xbh7mQXaizc36ula0... sync.1rx.io text/ht... 1
RX-734afebf-6edf-4bd3-a5b0-7e5... sync.targeting.unrulymedia.com gif 1
xuid?mid=2711&xuid=k-c13i_ng_4x... eb2.3lift.com gif 1
pixelCt.tpmn?tpmn_nid=26a68101... ad.tpmn.co.kr / Redir... 1
um?eid=80&uid=k-GNaed3g_4xbh... criteo-sync.teads.tv gif 1
img?mt_exid=10103&redirect=http... sync.mathtag.com gif / R... 1
act analytics.tiktok.com ping 1
pixel analytics.tiktok.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
p tr.snapchat.com ping 1
act analytics.tiktok.com ping 1
p tr6.snapchat.com ping 1
pixel analytics.tiktok.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
scevent.min.js sc-static.net script 1
p tr6.snapchat.com ping 1
p tr.snapchat.com ping 1
p tr.snapchat.com ping 1
p tr6.snapchat.com ping 1
act analytics.tiktok.com ping 1
pixel analytics.tiktok.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
scevent.min.js sc-static.net script 1
p tr.snapchat.com ping 1
p tr.snapchat.com ping 1
act analytics.tiktok.com ping 1
p tr6.snapchat.com ping 1
pixel analytics.tiktok.com ping 1
p?pid=fafb3cb3-1986-4442-95be... tr.snapchat.com png 1
events.js?sdkid=C4TUCNP6H18A0... analytics.tiktok.com script 1
scevent.min.js sc-static.net script 1
p tr.snapchat.com ping 1
cross-domain-bridge.html app.usercentrics.eu docu... 0
i api.avo.app preflig... 0
cross-domain-bridge.html app.usercentrics.eu docu... 0
syncframe?topUrl=www.fender.co... gum.criteo.com docu... 0
ingest pixels.spotify.com preflig... 0
2306 / 3166 requests
69.4 MB / 77.5 MB transferred
195 MB / 248 MB resources
Finish: 2 min
DOM
Console
What's new
AI assistance
What's new in DevTools 135

38. The screenshot above shows the "Network" tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user's browser and various third-party websites while the user visited and interacted with Defendant's Website at https://www.fender.com. The screenshot depicts only network traffic occurring ***after*** the user declined or rejected all such cookies by adjusting the "Do not sell my personal information" toggle switch on the popup cookie consent banner. As shown above, despite the user's declination or rejection of cookies, or at least all personalized advertising, analytics, and social media cookies, as well as all those cookies associated with the sale or sharing of users' personal information, the user's interactions with the Website resulted in the user's browser making a large number of GET and POST HTTP requests to third party web domains like www.facebook.com, analytics.google.com, analytics.tiktok.com, and many others. As further shown in the right-hand column of the screenshot, the user's browser sent cookies along with those HTTP requests to the third parties. This screenshot demonstrates that Defendant caused third-party cookie data and users' Private Communications to be transmitted to Third Parties, even after consumers declined or rejected all such cookies and tracking technologies, as well as the sale or sharing of their personal information, by adjusting the "Do not sell my personal information" toggle switch. All of these network calls are made to the Third Parties without the user's knowledge, and despite the user's declination or rejection of all such cookies.

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

40. As users interact with the Website, even after adjusting the "Do not sell my personal information" toggle switch, thereby declining or rejecting the use of cookies and similar technologies, including for personalized advertising, analytics, and social media, as well as the sale or sharing of the user's personal information with third parties for such functions, or other purposes, more data regarding users' behavior and communications are sent to third parties,

alongside the cookie data. The third-party cookies that Defendant wrongfully allows to be stored on users' devices and browsers, and to be transmitted to the Third Parties, cause the Third Parties to track and collect data on users' behaviors and communications, including Private Communications, on the Website. Because third-party cookies cause the Third Parties to track users' behavior across the Internet and across time, user data can be correlated and combined with other data sets to compile comprehensive user profiles that reflect consumers' behavior, preferences, and demographics (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes). These Third Parties monetize user profiles for advertising, sales, and marketing purposes to generate revenue and target advertising to Internet users. Advertisers can gain deep understanding of users' behavioral traits and characteristics and target those users with advertisements tailored to their consumer profiles and audience segments.

41. The Third Parties' code that the Website causes to be loaded and executed by the user's browser constitutes a wiretap because, when it is executed, it causes the Third Parties—separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. When the Third Parties use their respective wiretaps on Website users' Private Communications, the wiretaps are not like tape recorders or "tools" used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

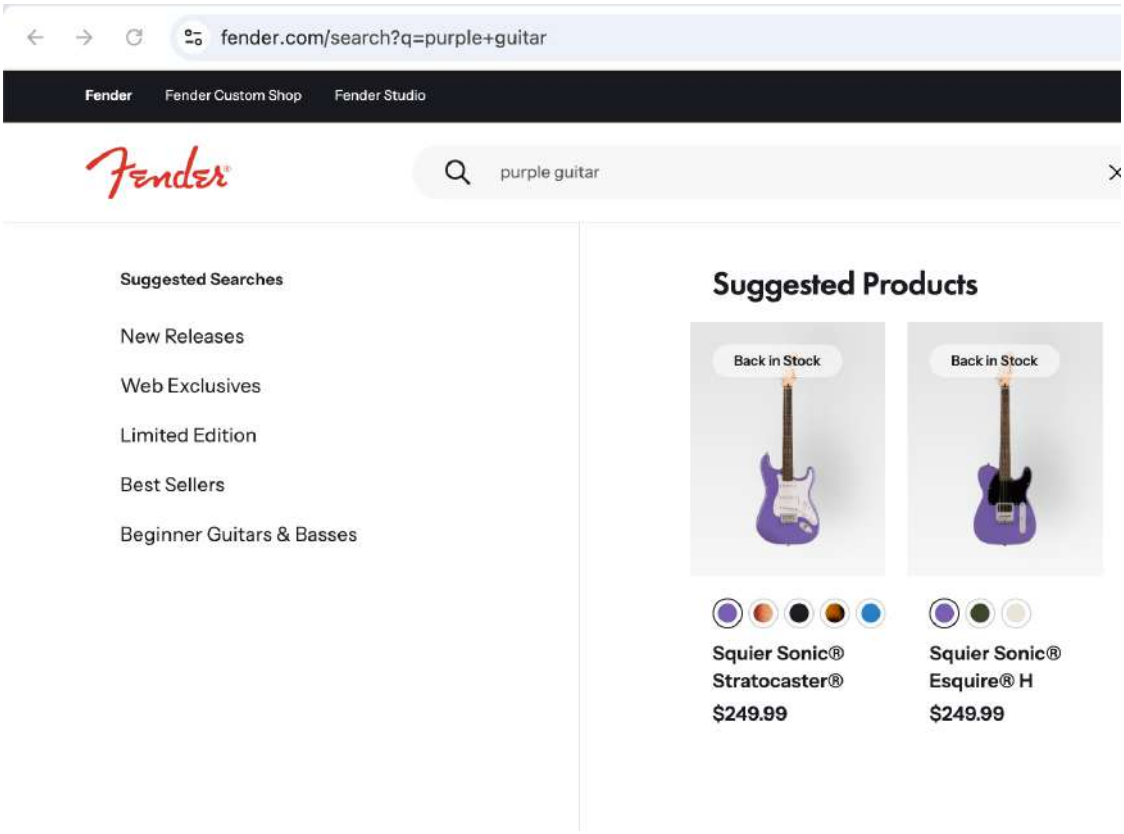
C. The Private Communications Intercepted and Collected Through Third-Party Cookies on Defendant's Website.[2]

1. The Website Causes the Interception of the Contents of Communications.

42. The Website includes a search function that allows users to search for products and related content. For example, a user interested in a particular product may enter the search term "purple guitar" into the Website's search field. When the user submits that search, the

[2] This section contains multiple examples of specific data being sent from a user's browser to third parties. Each example was collected after the user had declined or rejected cookies and tracking technologies in use on the Website, including those used for personalized advertising, analytics, and social media.

Website generates and loads a URL reflecting the user's search query, such as: https://www.fender.com/search?q=purple+guitar as shown in the following example screenshot:



43. When users enter information into the Website's search field, they intend to communicate the contents of their searches directly to Defendant for the purpose of obtaining information responsive to their queries.

44. Defendant programmed the Website such that URLs generated by users' searches—including URLs containing the users' search terms—are transmitted to Third Parties. As shown in the following sections, the Website caused such URLs (including, without limitation, URLs containing search strings) to be sent to Third Parties even after users rejected all unnecessary cookies through the Website's cookie-consent mechanism. Because the URLs contained users' search queries, the Third Parties were able to receive and learn the contents of those communications without users' knowledge or consent.

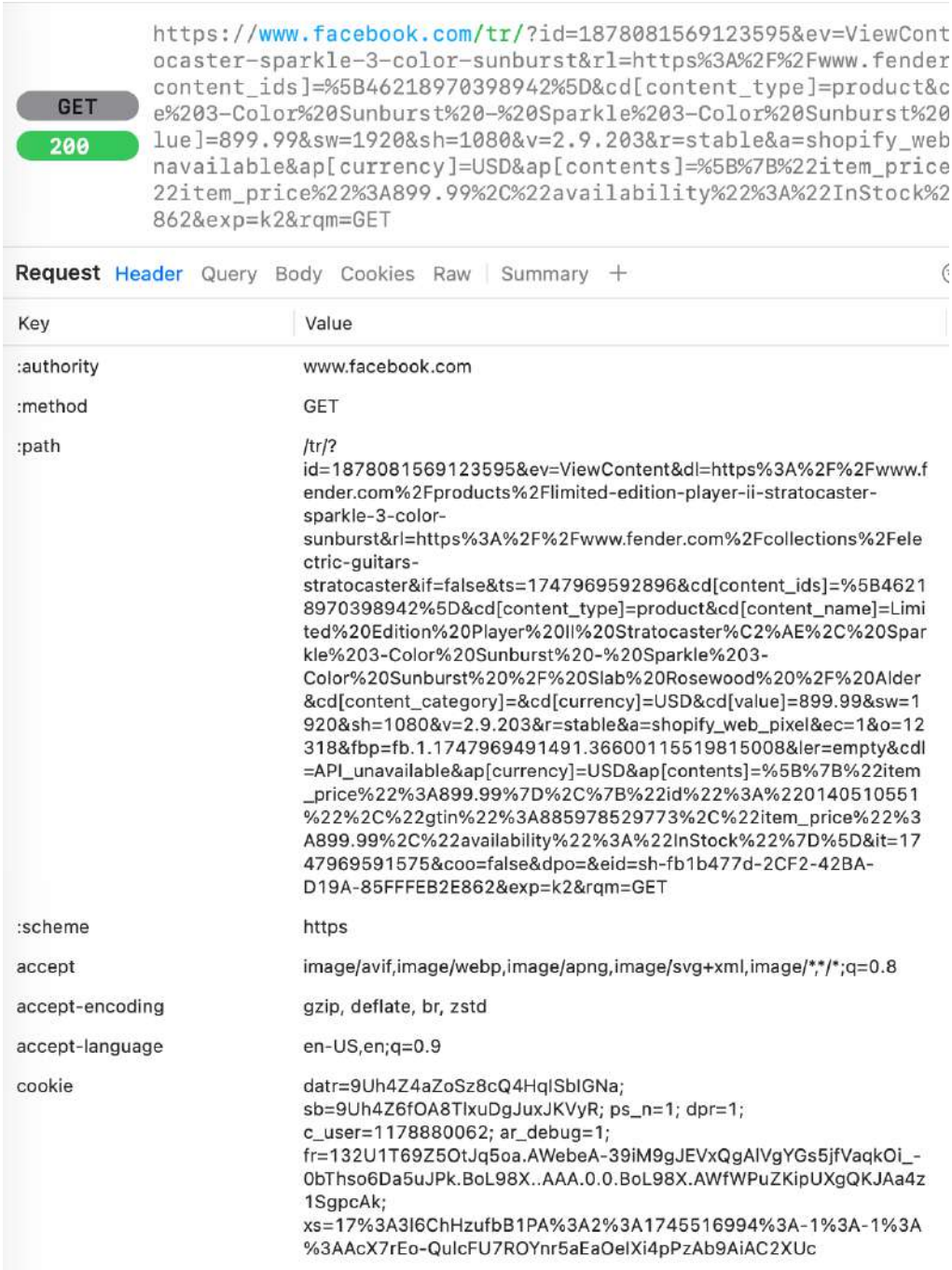
2. Facebook Cookies.

45. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices, even after users adjust the "Do not sell my personal information" toggle switch to reject cookies, to and from the **facebook.com** domain. This domain is associated with Meta's digital advertising and analytics platform that collects user information via cookies to assist Meta in performing data collection, behavioral analysis, user retargeting, and analytics.[3] Meta serves targeted ads to web users across Meta's ad network, which spans millions of websites and apps. Defendant specifically identified Facebook as a provider of "Marketing and Advertising" and "Performance & Analytics" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

46. Facebook's cookies help Meta track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. For example, the Website causes the following type of data to be sent to Meta when a user views a product on the Website after rejecting all unnecessary cookies:

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

[3] https://www.facebook.com/privacy/policies/cookies/.



GET
200

https://www.facebook.com/tr/?id=1878081569123595&ev=ViewCont
ocaster-sparkle-3-color-sunburst&rl=https%3A%2F%2Fwww.fender
content_ids]=%5B46218970398942%5D&cd[content_type]=product&c
e%203-Color%20Sunburst%20-%20Sparkle%203-Color%20Sunburst%20
lue]=899.99&sw=1920&sh=1080&v=2.9.203&r=stable&a=shopify_web
navailable&ap[currency]=USD&ap[contents]=%5B%7B%22item_price
22item_price%22%3A899.99%2C%22availability%22%3A%22InStock%2
862&exp=k2&rqm=GET

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	www.facebook.com
:method	GET
:path	/tr/?id=1878081569123595&ev=ViewContent&dl=https%3A%2F%2Fwww.fender.com%2Fproducts%2Flimited-edition-player-ii-stratocaster-sparkle-3-color-sunburst&rl=https%3A%2F%2Fwww.fender.com%2Fcollections%2Felectric-guitars-stratocaster&if=false&ts=1747969592896&cd[content_ids]=%5B462188970398942%5D&cd[content_type]=product&cd[content_name]=Limited%20Edition%20Player%20II%20Stratocaster%C2%AE%2C%20Sparkle%203-Color%20Sunburst%20-%20Sparkle%203-Color%20Sunburst%20%2F%20Slab%20Rosewood%20%2F%20Alder&cd[content_category]=&cd[currency]=USD&cd[value]=899.99&sw=1920&sh=1080&v=2.9.203&r=stable&a=shopify_web_pixel&ec=1&o=12318&fbp=fb.1.1747969491491.366001155198150 08&ler=empty&cdl=API_unavailable&ap[currency]=USD&ap[contents]=%5B%7B%22item_price%22%3A899.99%7D%2C%7B%22id%22%3A%220140510551%22%2C%22gtin%22%3A885978529773%2C%22item_price%22%3A899.99%2C%22availability%22%3A%22InStock%22%7D%5D&it=1747969591575&coo=false&dpo=&eid=sh-fb1b477d-2CF2-42BA-D19A-85FFFEB2E862&exp=k2&rqm=GET
:scheme	https
accept	image/avif,image/webp,image/apng,image/svg+xml,image/*;*/*;q=0.8
accept-encoding	gzip, deflate, br, zstd
accept-language	en-US,en;q=0.9
cookie	datr=9Uh4Z4aZoSz8cQ4HqlSbIGNa; sb=9Uh4Z6fOA8TlxuDgJuxJKVyR; ps_n=1; dpr=1; c_user=1178880062; ar_debug=1; fr=132U1T69Z5OtJq5oa.AWebeA-39iM9gJEVxQgAlVgYGs5jfVaqkOi_-0bThso6Da5uJPk.BoL98X..AAA.0.0.BoL98X.AWfWPuZKipUXgQKJAa4z1SgpcAk; xs=17%3A3l6ChHzufbB1PA%3A2%3A1745516994%3A-1%3A-1%3A%3AAcX7rEo-QulcFU7ROYnr5aEaOelXi4pPzAb9AiAC2XUc

dnt	1
priority	i
referer	https://www.fender.com/
sec-ch-ua	"Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
sec-fetch-dest	image
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
sec-fetch-storage-access	active
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Host	www.facebook.com

GET
200

https://www.facebook.com/tr/?id=1878081569123595&ev=ViewContocaster-sparkle-3-color-sunburst&rl=https%3A%2F%2Fwww.fendercontent_ids]=%5B46218970398942%5D&cd[content_type]=product&ce%203-Color%20Sunburst%20-%20Sparkle%203-Color%20Sunburst%20lue]=899.99&sw=1920&sh=1080&v=2.9.203&r=stable&a=shopify_webnavailable&ap[currency]=USD&ap[contents]=%5B%7B%22item_price22item_price%22%3A899.99%2C%22availability%22%3A%22InStock%2862&exp=k2&rqm=GET

Request Header Query Body Cookies Raw Summary +

Key	Value
a	shopify_web_pixel
ap[contents]	%5B%7B"item_price"%3A899.99%7D%2C%7B"id"%3A"0140510551"%2C"gtin"%3A885978529773%2C"item_price"%3A899.99%2C"availability"%3A"InStock"%7D%5D
ap[currency]	USD
cd[content_category]	
cd[content_ids]	%5B46218970398942%5D
cd[content_name]	Limited%20Edition%20Player%20II%20Stratocaster%C2%AE%2C%20Sparkle%203-Color%20Sunburst%20-%20Sparkle%203-Color%20Sunburst%20%2F%20Slab%20Rosewood%20%2F%20Alder
cd[content_type]	product
cd[currency]	USD
cd[value]	899.99
cdl	API_unavailable
coo	false
dl	https%3A%2F%2Fwww.fender.com%2Fproducts%2Flimited-edition-player-ii-stratocaster-sparkle-3-color-sunburst

dpo	
ec	1
eid	sh-fb1b477d-2CF2-42BA-D19A-85FFFEB2E862
ev	ViewContent
exp	k2
fbp	fb.1.1747969491491.36600115519815008
id	1878081569123595
if	false
it	1747969591575
ler	empty
o	12318
r	stable
rl	https%3A%2F%2Fwww.fender.com%2Fcollections%2Felectric-guitars-stratocaster
rqm	GET
sh	1080
sw	1920
ts	1747969592896
v	2.9.203

47. The "referer" header discloses to Facebook that the user was browsing the Website, at https://www.fender.com. The "user-agent" header enables Facebook to determine the user's device type, operating system, and browser. In addition, though not depicted above, the Website causes the user's IP address to be transmitted to Facebook, further enabling Facebook to track the user and identify the user's geolocation.

48. The parameters above starting with "cd" are "custom dimension" parameters. Here, the "cd" parameters disclose to Facebook that the user was viewing a Fender Limited Edition Player II Stratocaster, with a sparkle sunburst color, and that the product cost $899.99. The "ev" parameter is short for "event." In this instance, the event is a "ViewContent."

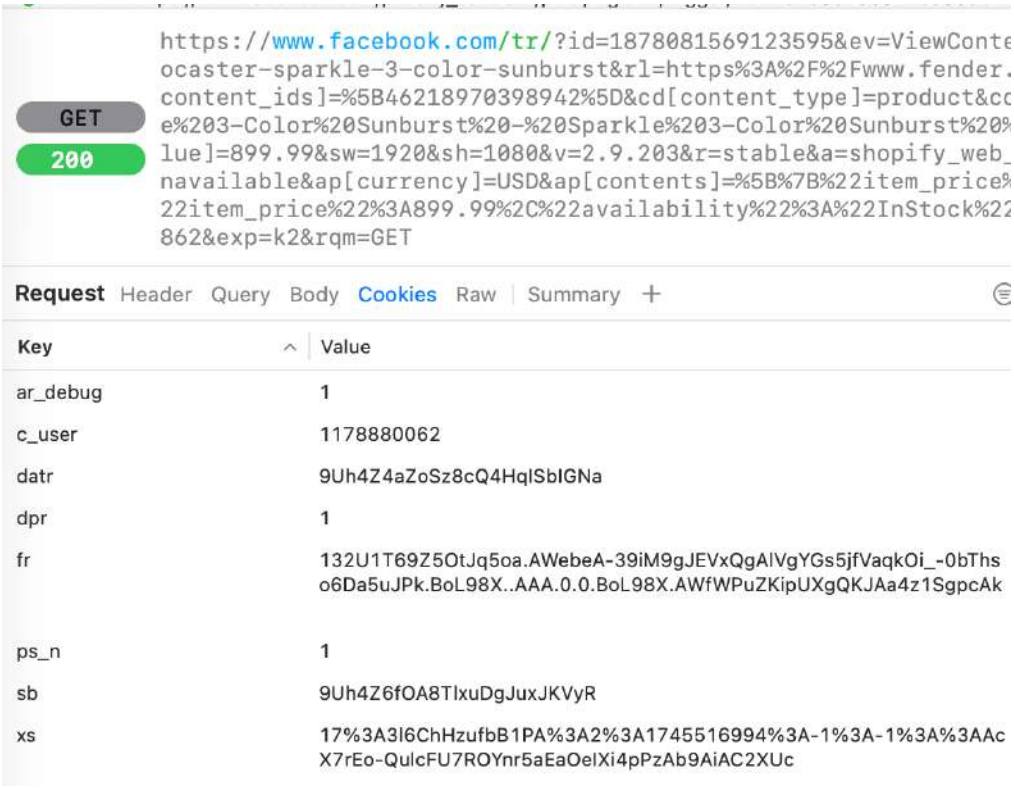
49. The "dl" parameter refers to "Document Location." It tells Facebook the specific webpage on which the Event occurred – in this case it discloses to Meta the full URL that the user was viewing. To the extent user search queries were contained in the URL, they would be sent to Meta.

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

51. The "sw" and "sh" parameters stand for "screen width" and "screen height," and correspond to the display the user was viewing when the event was recorded.

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

53. Cookies are sent along with all data transmissions to Meta. For instance, the following cookies were sent along with the ViewContent event:



54. Among these cookies is the "c_user" cookie, which enables Facebook to identify a specific user when they are logged in to their account. The "c_user "cookie stores a user's unique ID, which is associated with their Facebook profile. This ID enables Facebook to track user interactions on its platform and across sites that use Facebook plugins, such as adding items to a cart, clicking "Like" buttons, or engaging with comment sections. When combined with other data sent to the Facebook domain, this cookie allows Meta to track users' browsing activities. Facebook uses this data for various purposes, such as personalizing content, enhancing ad targeting accuracy, and refining its user experience.

55. In particular, by identifying users who have shown interest in certain products or content, the facebook.com cookies enable Meta's advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Meta's ad network.[4] These cookies allow Meta to collect data on how users interact with websites, regardless of whether they have a Facebook account or are logged in.[5]

56. The facebook.com cookies allow Meta to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses, which allow Defendant to determine whether a user is located in California).[6]

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

[4] *Id.*; https://allaboutcookies.org/what-data-does-facebook-collect.
[5] https://allaboutcookies.org/what-data-does-facebook-collect.
[6] *Id.*

3. Google Cookies.

58. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices, even after users adjust the "Do not sell my personal information" toggle switch to reject cookies, to and from the **www.youtube.com**, **play.google.com**, **analytics.google.com**, and **www.google.com** domains. Each of these domains is associated with Google LLC's digital advertising and analytics platform that collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.[7] Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's DoubleClick cookies.[8] Google's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. Further, by identifying users who have shown interest in certain products or content, Google's cookies enable its advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Google's ad network.[9]

59. Google sends cookies when a web user visits a webpage that shows Google Marketing Platform advertising products and/or Google Ad Manager ads.[10] "Pages with Google Marketing Platform advertising products or Google Ad Manager ads include ad tags that instruct browsers to request ad content from [Google's] servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google Marketing Platform advertising products or Google Ad Manager ads for this to happen; it just needs to include Google Marketing

[7] *See* Our advertising and measurement cookies (available at https://business.safety.google/adscookies/).
[8] *See, e.g.* https://www.ghostery.com/whotracksme/trackers/doubleclick.
[9] *See, e.g.* About cross-channel remarketing in Search Ads 360 (available at https://support.google.com/searchads/answer/7189623?hl=en); About dynamic remarketing for retail (available at https://support.google.com/google-ads/answer/6099158?hl=en&sjid=11962135750754589 08-NC).
[10] *See* How Google Marketing Platform advertising products and Google Ad Manager use cookies (available at https://support.google.com/searchads/answer/2839090?hl=en&sjid=11962135750754589 08-NC); *see also* Cookies and user identification (available at https://developers.google.com/tag-platform/security/concepts/cookies).

Platform advertising products or Google Ad Manager ad tags, which might load a click tracker or impression pixel instead." *Id.* As Google explains, "Google Marketing Platform advertising products and Google Ad Manager send a cookie to the browser after any impression, click, or other activity that results in a call to our servers." *Id.*

60. Google also uses cookies in performing analytical functions. As Google explains, "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es]."[11] "To measure a website … [one] add[s] a small piece of JavaScript measurement code to each page on [a] site." *Id.* Then, "[e]very time a user visits a webpage, the tracking code will collect … information about how that user interacted with the page." *Id.* Google Analytics enables website owners to "measure when someone loads a page, clicks a link, [ ] makes a purchase;" "completes a purchase"; "searches [] website or app"; "select content on [] website or app"; "views an item"; and "views their shopping cart."[12]

61. Defendant specifically identified Google as a provider of "Marketing and Advertising" and "Performance & Analytics" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

62. Google's cookies allow it to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data, including whether a user is located in California.[13]

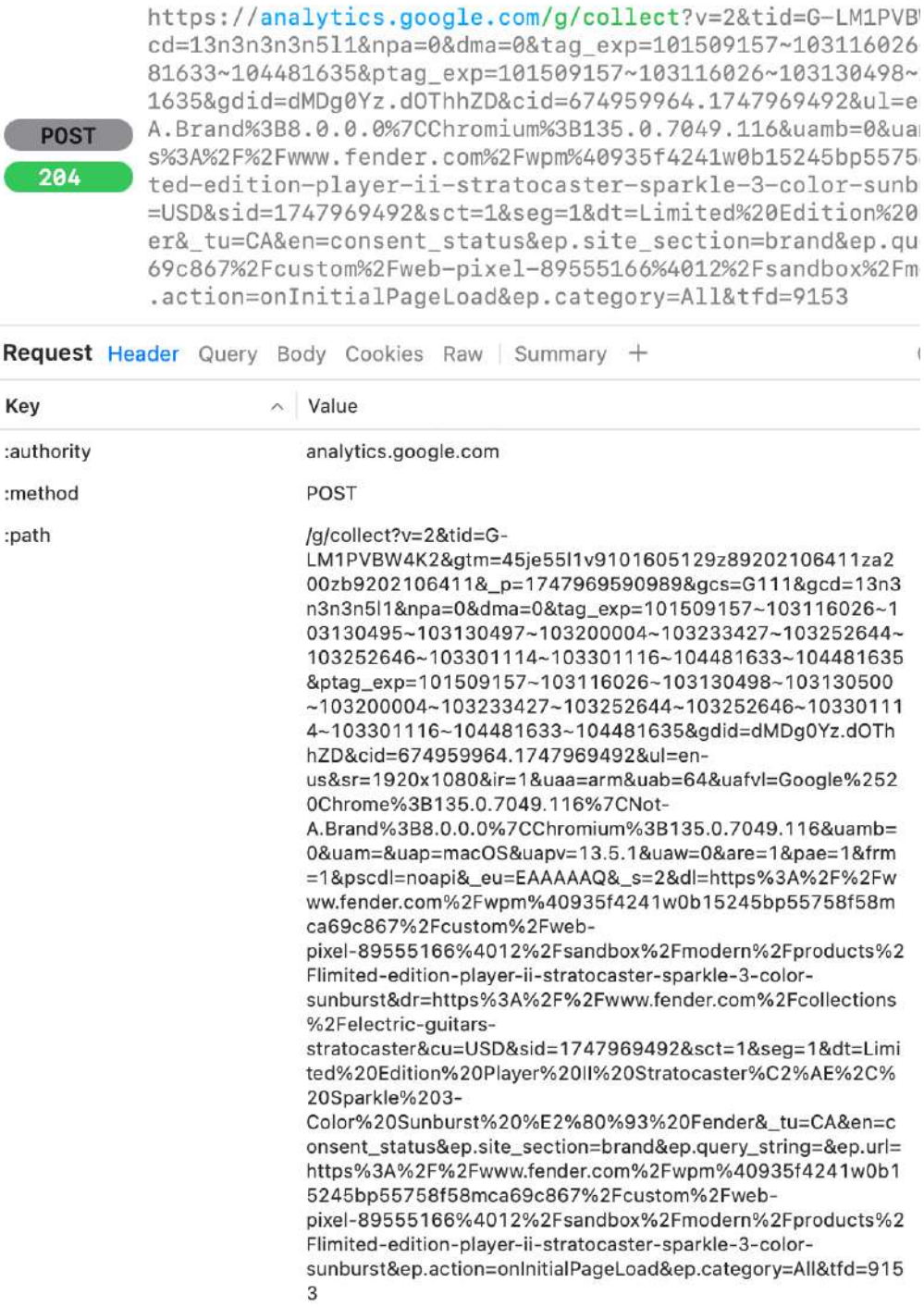
---

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

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

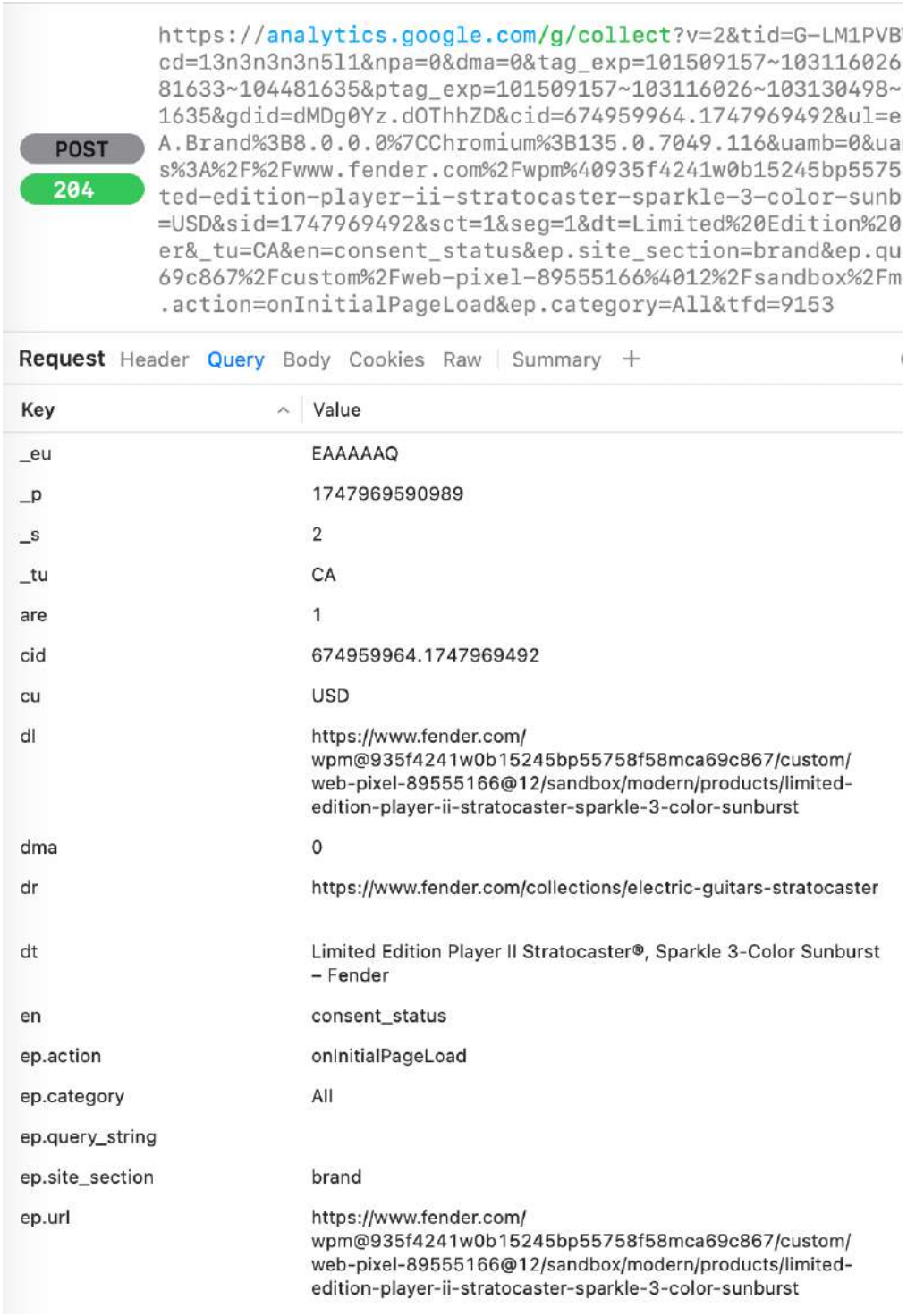
[13] *See* About the Google Tag (available at https://support.google.com/searchads/answer/7550511?hl=en); How Floodlight Recognizes Users (available at https://support.google.com/searchads/answer/2903014?hl=en); How Google Ads tracks website conversions (available at https://support.google.com/google-ads/answer/7521212);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

63. For example, the Google software code that Defendant causes to be stored on and executed by the Website user's device causes the following data to be sent to Google's domain, at analytics.google.com:



(available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://support.google.com/analytics/answer/9267735).

:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br, zstd
accept-language	en-US,en;q=0.9
content-length	0
cookie	__Secure-3PAPISID=-FcNj0U0rp9hxuEG/AYo9LFEwi8KFnkCW5; __Secure-3PSID=g.a000xAiz-pTWKStsux6ulivu2L9zLBGyGfQsnI3V9ixLi_RWZ0B0eR_c_Kslx0U-5B13ogOaCgACgYKAeASARYSFQHGX2Miwj5r3roLc3QOmUeqKq4szBoVAUF8yKqde6kJcwhhD6MkoR8F0rCx0076; NID=524=LokPuvR8vl0vAUNB_M8fLnmlOlRpzWHsrSWI9rzXleFJBbXWVzzbA0pr89KUUqdXryy1c0rhCDQGAdkrqyCkg4nj0VbRCYkzOcON33EXiTUZ-Sm71zCNE1gVitOnbG_vh1jG2N1WLD5vKyE4BhJqrDZFeaUkPcxtQ2-Nr-xxOmeR7BTYpzFLQtp4aMMVQL5VVZ8xylu3OgcwwvaLVZH-RsXpmvwS-TiUAsCSwqZnNx1DFSXsupniZxfZveeE-2edGbWUvj_YW6HOpIp4KFFHZ308C3MS38LElLy2CkAV68SfPvziE6WlMjcL8qe_WLyMSQ6LvbIpr-45t3HYLpT9ng6OcChtdHF9WcvnspDqIfq_ed6XqZQ; __Secure-3PSIDTS=sidts-CjEBjpIskDyRDzvBO8FOxvqi6TO6vFVJWccK1Ely9_Tv1UY1_SIp5t1eV6XoZzp71uW8EAA; __Secure-3PSIDCC=AKEyXzXnzhx7qs-RFhkKgX4SUzX4yz2BucsE2vud0gbP9qdM-sJhCONTg52yPlVZ_GsmJFZInuo
dnt	1
Host	analytics.google.com
origin	null
priority	u=1, i
sec-ch-ua	"Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
sec-fetch-dest	empty
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
sec-fetch-storage-access	active
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
x-client-data	CJe2yQEIo7bJAQipncoBCPvsygEIk6HLAQiSo8sBCIagzQEIucjNAQje7s4B



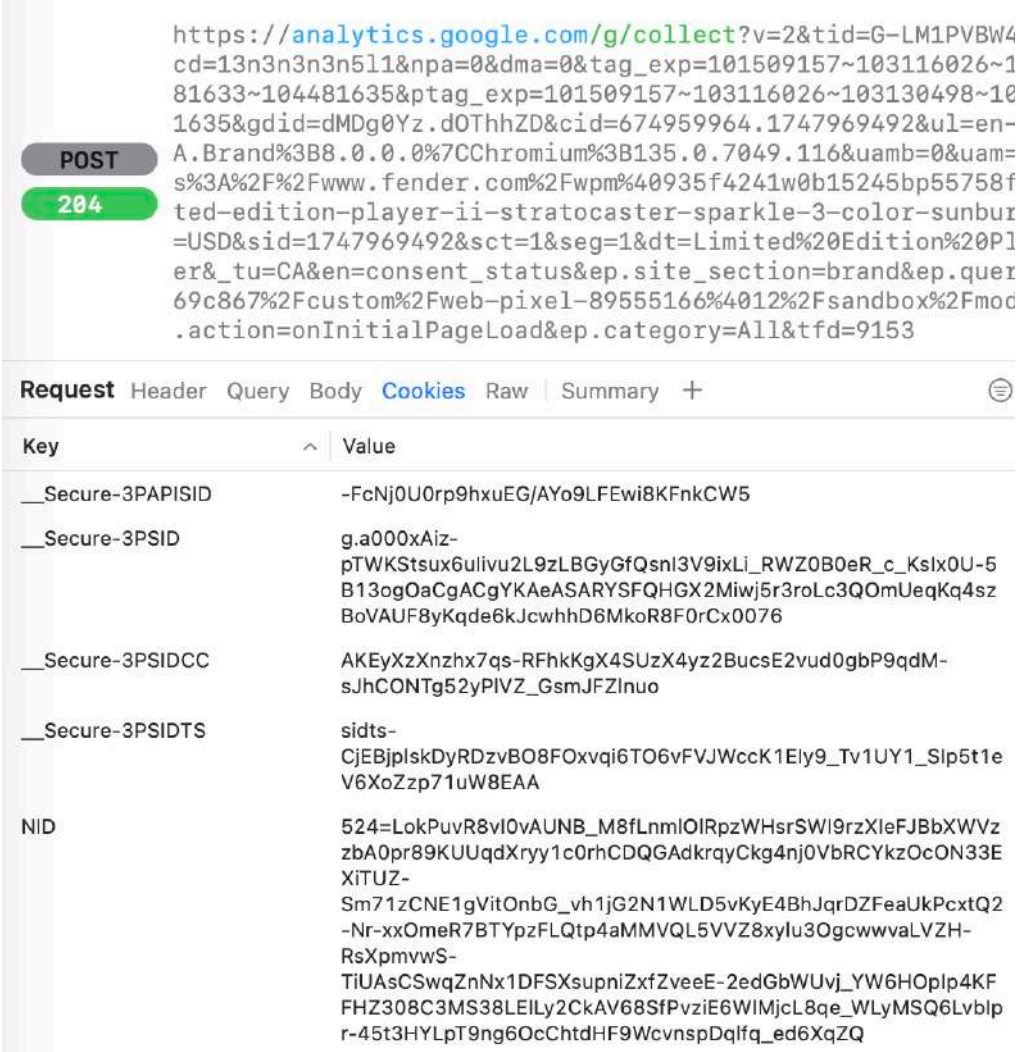
POST
204

https://analytics.google.com/g/collect?v=2&tid=G-LM1PVB
cd=13n3n3n3n5l1&npa=0&dma=0&tag_exp=101509157~103116026
81633~104481635&ptag_exp=101509157~103116026~103130498~
1635&gdid=dMDg0Yz.dOThhZD&cid=674959964.1747969492&ul=e
A.Brand%3B8.0.0.0%7CChromium%3B135.0.7049.116&uamb=0&ua
s%3A%2F%2Fwww.fender.com%2Fwpm%40935f4241w0b15245bp5575
ted-edition-player-ii-stratocaster-sparkle-3-color-sunb
=USD&sid=1747969492&sct=1&seg=1&dt=Limited%20Edition%20
er&_tu=CA&en=consent_status&ep.site_section=brand&ep.qu
69c867%2Fcustom%2Fweb-pixel-89555166%4012%2Fsandbox%2Fm
.action=onInitialPageLoad&ep.category=All&tfd=9153

Request Header Query Body Cookies Raw Summary +

Key	Value
_eu	EAAAAAQ
_p	1747969590989
_s	2
_tu	CA
are	1
cid	674959964.1747969492
cu	USD
dl	https://www.fender.com/wpm@935f4241w0b15245bp55758f58mca69c867/custom/web-pixel-89555166@12/sandbox/modern/products/limited-edition-player-ii-stratocaster-sparkle-3-color-sunburst
dma	0
dr	https://www.fender.com/collections/electric-guitars-stratocaster
dt	Limited Edition Player II Stratocaster®, Sparkle 3-Color Sunburst – Fender
en	consent_status
ep.action	onInitialPageLoad
ep.category	All
ep.query_string	
ep.site_section	brand
ep.url	https://www.fender.com/wpm@935f4241w0b15245bp55758f58mca69c867/custom/web-pixel-89555166@12/sandbox/modern/products/limited-edition-player-ii-stratocaster-sparkle-3-color-sunburst

frm	1
gcd	13n3n3n3n5l1
gcs	G111
gdid	dMDg0Yz.dOThhZD
gtm	45je55l1v9101605129z89202106411za200zb9202106411
ir	1
npa	0
pae	1
pscdl	noapi
ptag_exp	101509157~103116026~103130498~103130500~103200004~103233427~103252644~103252646~103301114~103301116~104481633~104481635
sct	1
seg	1
sid	1747969492
sr	1920x1080
tag_exp	101509157~103116026~103130495~103130497~103200004~103233427~103252644~103252646~103301114~103301116~104481633~104481635
tfd	9153
tid	G-LM1PVBW4K2
uaa	arm
uab	64
uafvl	Google%20Chrome;135.0.7049.116|Not-A.Brand;8.0.0.0|Chromium;135.0.7049.116
uam	
uamb	0
uap	macOS
uapv	13.5.1
uaw	0
ul	en-us
v	2



64. As with the data sent to Facebook, the data sent to Google includes the "referer" and "user-agent" headers, as well as the user's IP address.

65. Further, the data sent to google includes the "dl" parameter, which stands for "document location." This parameter discloses to Google the exact URL that the user was visiting on the website (i.e., https://www.fender.com/wpm@935f4241w0b15245bp55758f58mca69c867/custom/web-pixel-89555166@12/sandbox/modern/products/limited-edition-player-ii-stratocaster-sparkle-3-color-sunburst) The data also includes the "dt" or "document title" parameter, which is the title of the page the user is viewing: "Limited Edition Player II Stratocaster®, Sparkle 3-Color Sunburst – Fender." To the extent user search queries were contained in the URL, they would be sent to Google.

66. The "npa" parameter refers to "Non-Personalized Ads." When npa is set to 1, it indicates non-personalized ads preference is enabled. Here, npa is set to 0, indicating that standard (personalized) ads are enabled.

67. The parameters beginning in "ua…" tell Google extensive information about the user's device and browser, including the specific operating system, browser brand, and device processor.

68. The "cid" parameter above refers to "Client ID." It contains a unique identifier for the user's browser and device, that enables Google to link the user to their interactions with the website.[14]

69. The data also includes cookies. The "NID" cookie is used for Google advertising. According to Google documentation, "[t]he 'NID' cookie is used to show Google ads in Google services for signed-out users," and "expires 6 months after a user's last use."[15]

70. The "__Secure-3PAPISID" and "__Secure-3PSID" cookies used on the Website are utilized by Google to build a profile of Website visitor interests to show relevant and personalized ads through retargeting.

71. Because Google's cookies operate across multiple sites (i.e., cross-site tracking), the cookie enables Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google's advertising platform aggregates user data to create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics and audience segments based on shared traits (such as females, Millennials, etc.), and to perform targeted advertising and marketing analytics.

72. Thus, the Google cookies used on the Website enable Google to track users' interactions with advertisements to help advertisers understand how users engage with ads across different websites. Further, the user data collected through the cookie enables the delivery of

[14] *See, e.g.*, https://cheatography.com/dmpg-tom/cheat-sheets/google-universal-analytics-url-collect-parameters/; https://www.analyticsmarket.com/blog/how-google-analytics-collects-data/; https://www.owox.com/blog/use-cases/google-analytics-client-id/.

[15] https://policies.google.com/technologies/cookies?hl=en-US.

personalized ads based on user interests and behaviors. For instance, if a user frequently visits travel-related websites, Google will show them more travel-related advertisements. Further, the collected data is used to generate reports for advertisers, helping them assess the performance of their ad campaigns and make data-driven decisions (such as renaming their products). Further, Google's advertising platform enables advertisers to retarget marketing, which Google explains allows advertisers to "show previous visitors ads based on products or services they viewed on your website. With messages tailored to your audience, dynamic remarketing helps you build leads and sales by bringing previous visitors back to your website to complete what they started."[16]

73. Further, in its "Shared Data Under Measurement Controller-Controller Data Protection Terms," Google states: "Google can access and analyze the Analytics data customers share with us to better understand online behavior and trends, and improve our products and services—for example, to improve Google search results, detect and remove invalid advertising traffic in Google Ads, and test algorithms and build models that power services like Google Analytics Intelligence that apply machine-learning to surface suggestions and insights for customers based on their analytics data and like Google Ads that applies broad models to improve ads personalization and relevance. These capabilities are critical to the value of the products we deliver to customers today."[17] Thus, Google can have the capability to use the data it collects for understanding online behavior and trends, machine learning, and improving its own products and services.

4. TikTok Cookies.

74. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices, even after users adjust the "Do not sell my personal information" toggle switch to reject cookies, to and from the **analytics.tiktok.com** domain. This domain is associated with TikTok for Business, a suite of tools offered by TikTok, a social media platform owned by

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

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

ByteDance Ltd., known for short-form video sharing. The TikTok platform is used to create and share videos, and it utilizes cookies for various purposes including assisting brands and marketers to create, manage, and optimize ad campaigns on the platform.[18]

75. Defendant specifically identified TikTok as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

76. TikTok utilizes analytics.tiktok.com cookies to collect data on user interactions with websites that have integrated TikTok's tracking technologies (such as the Website). These cookies are used to "measure and improve the performance of your advertising campaigns and to personalize the user's experience (including ads) on TikTok."[19] TikTok further explains that it uses cookies to "match events with people who engage with your content on TikTok. Matched events are used to improve measurement and optimize ad campaigns. They can also contribute to building your retargeting and engagement audiences." *Id.* These cookies enable TikTok to recognize and track users across different sessions and domains (i.e., cross-site tracking) and to collect and synchronize user data to observe and evaluate TikTok user behavior.

77. These cookies enable TikTok to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, including *email addresses and phone numbers*; (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) session information, (x) user identifiers, and (xi) geolocation data in the form of the IP address, including whether a user is located in California.[20]

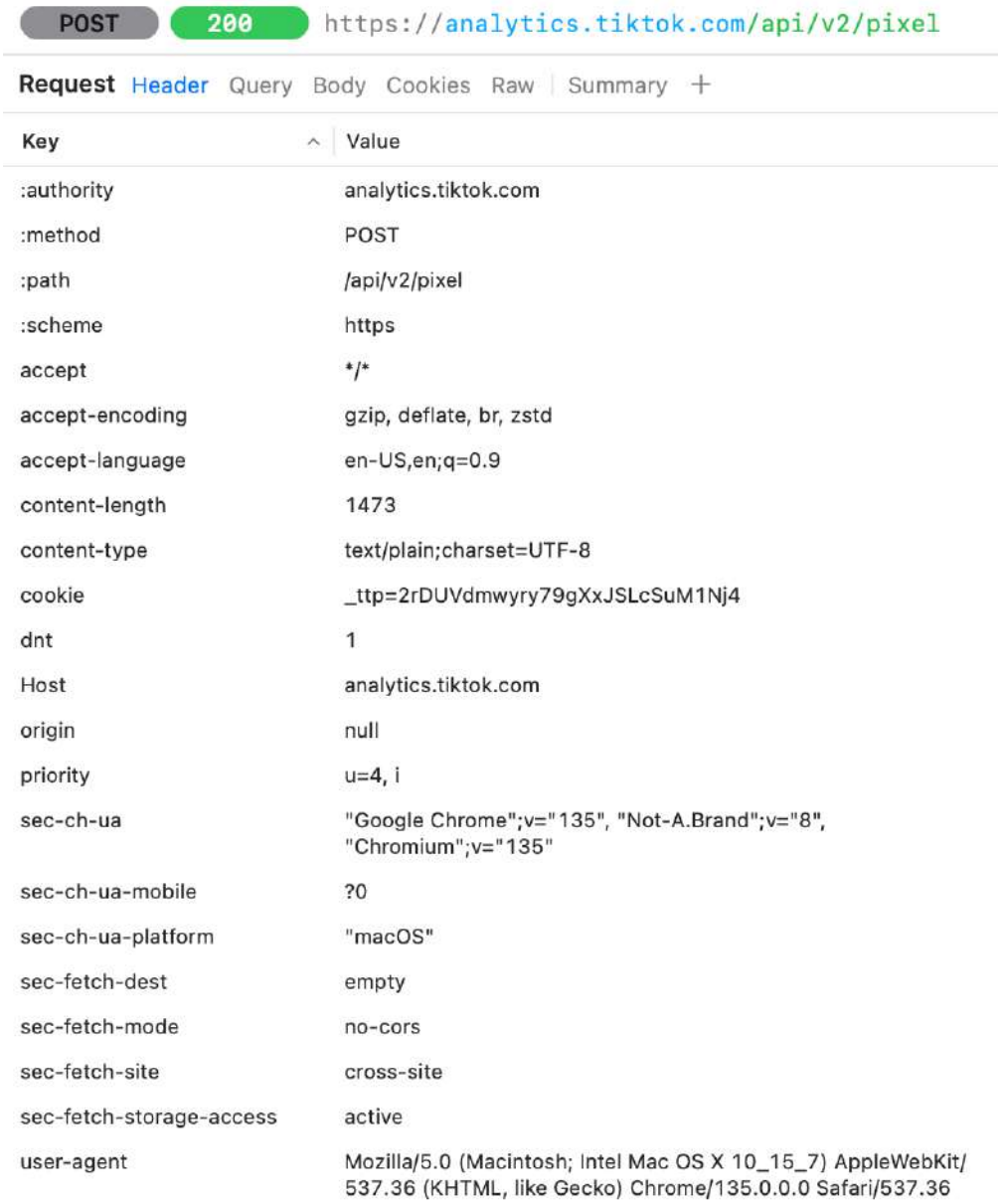
---

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

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

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

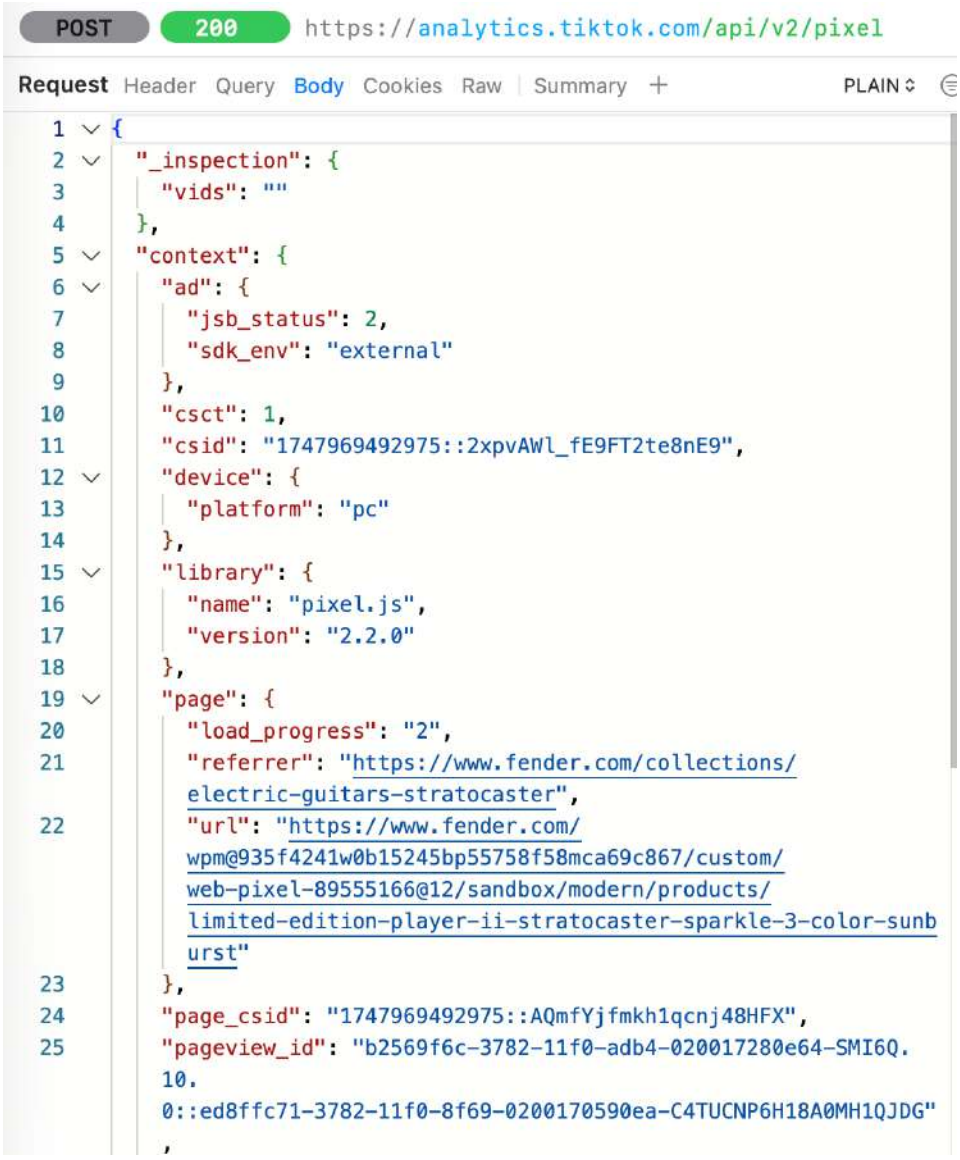
78. For example, the TikTok software code that Defendant causes to be stored on and executed by the Website user's device causes the following data to be sent to TikTok's domain, at https://analytics.tiktok.com:



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

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	analytics.tiktok.com
:method	POST
:path	/api/v2/pixel
:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br, zstd
accept-language	en-US,en;q=0.9
content-length	1473
content-type	text/plain;charset=UTF-8
cookie	_ttp=2rDUVdmwyry79gXxJSLcSuM1Nj4
dnt	1
Host	analytics.tiktok.com
origin	null
priority	u=4, i
sec-ch-ua	"Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
sec-fetch-dest	empty
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
sec-fetch-storage-access	active
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36

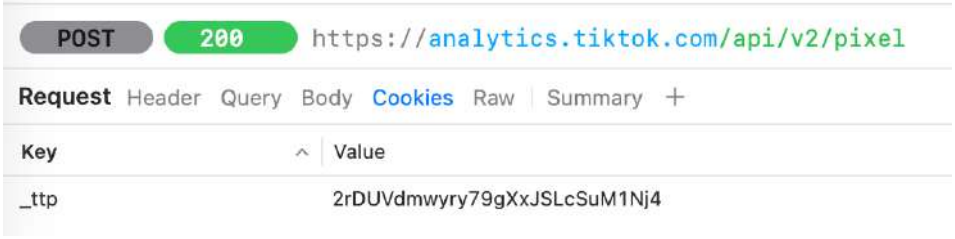


POST 200 https://analytics.tiktok.com/api/v2/pixel

Request Header Query Body Cookies Raw Summary + PLAIN


```
{
  "_inspection": {
    "vids": ""
  },
  "context": {
    "ad": {
      "jsb_status": 2,
      "sdk_env": "external"
    },
    "csct": 1,
    "csid": "1747969492975::2xpvAWl_fE9FT2te8nE9",
    "device": {
      "platform": "pc"
    },
    "library": {
      "name": "pixel.js",
      "version": "2.2.0"
    },
    "page": {
      "load_progress": "2",
      "referrer": "https://www.fender.com/collections/electric-guitars-stratocaster",
      "url": "https://www.fender.com/wpm@935f4241w0b15245bp55758f58mca69c867/custom/web-pixel-89555166@12/sandbox/modern/products/limited-edition-player-ii-stratocaster-sparkle-3-color-sunburst"
    },
    "page_csid": "1747969492975::AQmfYjfmkh1qcnj48HFX",
    "pageview_id": "b2569f6c-3782-11f0-adb4-020017280e64-SMI6Q.10.0::ed8ffc71-3782-11f0-8f69-0200170590ea-C4TUCNP6H18A0MH1QJDG"
    ,
```

```
    "pixel": {
      "code": "C4TUCNP6H18A0MH1QJDG",
      "runtime": "6"
    },
    "session_id":
    "b2569f6c-3782-11f0-adb4-020017280e64::rgEJajHjHy7gNii9fQZ1-C
    4TUCNP6H18A0MH1QJDG",
    "user": {
      "anonymous_id": "01JVXHKHZDCW8WTYMNHZ96FQYF_.tt.0"
    },
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X
    10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.
    0.0 Safari/537.36",
    "variation_id": "test_2_single_track"
  },
  "event": "Pageview",
  "event_id": "",
  "is_onsite": false,
  "message_id":
  "messageId-1747969592600-5249453025762-C4TUCNP6H18A0MH1QJDG",
  "properties": {},
  "signal_diagnostic_labels": {
    "hashed_email": {
      "label": "missing"
    },
    "hashed_phone": {
      "label": "missing"
    },
    "raw_auto_email": {
      "label": "missing"
    },
    "raw_auto_phone": {
      "label": "missing"
    },
    "raw_email": {
      "label": "missing"
    },
    "raw_phone": {
      "label": "missing"
    }
  },
  "timestamp": "2025-05-23T03:06:32.600Z"
}
```

79. In addition to the "referer" and "user-agent" headers depicted above (and the user's IP address, which is not depicted above), TikTok receives detailed information regarding the user's visits. For example, TikTok receives the full URL of the product page that the user was viewing. To the extent user search queries were contained in the URL, they would be sent to TikTok.

80. In addition, the Website causes the user's browser to send TikTok tracking information, even after the user has rejected all cookies. In particular, the data includes the "session_id," which is a unique identifier generated by TikTok to track a user's activity. This allows TikTok to correlate the user's behavior from a browsing session, including page views and conversions, to a particular user to enhance advertising measurement, attribution, and targeting.[21]

81. Along with this data, the TikTok software code that Defendant causes to be stored on and executed by the user's device causes the "_ttp" cookie to be sent to TikTok. According to TikTok's documentation, the "_ttp" cookie is one of the company's advertising cookies, the purpose of which is "[t]o measure and improve the performance of your advertising campaigns and to personalize the user's experience (including ads) on TikTok."[22]

82. By collecting this user data, TikTok performs user behavior tracking, i.e., monitoring user actions like page views, clicks, and interactions to understand user engagement; advertising optimization, i.e., gathering data to enhance the relevance and effectiveness of TikTok advertising campaigns; and performance measurement (i.e., assessing the success of marketing efforts by analyze user responses to ads and content).[23]

83. Further, TikTok's Automatic Advanced Matching feature functions as follows: "When a visitor lands on your website and inputs customer information during registration, sign-in, contact, or checkout on a website where you installed your pixel, Automatic Advanced

[21] *See, e.g.*, How to get TikTok session id? (available at https://gbtimes.com/how-to-get-tiktok-session-id/).
[22] *See* TikTok for Business: Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).
[23] *See* TikTok for Business: Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).

Matching will capture information from those fields. …TikTok will use hashed information to link event information to people on TikTok. Tiktok may use matched events to better attribute events to TikTok ads, optimize advertisers' future campaigns, and depending on advertisers' and users' settings, TikTok may also add people to advertisers' retargeting or engagement audiences."[24]

5. Microsoft Bing Cookies.

84. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices, even after users adjust the "Do not sell my personal information" toggle switch to reject cookies, to and from the **bing.com** domain and subdomains. "The webpage bat.bing.com is a host for Bing Ads Conversion tracking code. This webpage is owned by Microsoft[.]"[25] The domain is associated with Bing, Microsoft's search engine, as well as Microsoft's digital advertising and analytics platforms. When a webpage loads a bat.bing.com cookie, it "tells Microsoft Advertising about the user visits to [the] webpage."[26] Microsoft uses bat.bing.com cookies to "record[] what customers do on [a] website and send[] that information to Microsoft Advertising." [27] Microsoft then serves targeted ads to web users across its extensive ad networks, which utilizes its "rich" supply of gathered data to "reach more than a billion people[.]"[28]

85. Defendant specifically identified Microsoft as a provider of "Marketing and Advertising" and "Performance and Analytics" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

86. Bat.bing.com cookies collect consumers' (i) search history and browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information

[24] TikTok for Business: How to set up Automatic Advanced Matching (available at https://ads.tiktok.com/help/article/how-to-set-up-automatic-advanced-matching?lang=en).
[25] https://answers.microsoft.com/en-us/msadvs/forum/all/does-batbing-track-your-browser-searches-and-sites/0a402f00-60c2-4d54-bd7d-81b67ccc7f13.
[26]https://help.ads.microsoft.com/apex/index/3/en/56959#:~:text=The%20most%20important%20request%20is,making%20when%20your%20webpage%20loads.
[27] https://help.ads.microsoft.com/#apex/ads/en/56960/1.
[28] https://answers.microsoft.com/en-us/msadvs/forum/all/opt-out-of-audience-ads/753bc0fc-c04f-4e20-a94a-abaa950ccf31#:~:text=When%20you%20come%20to%20Microsoft,and%20rich%20first%2Dparty%20data.

(including zip code[29]; gender[30]; age[31] (including identifying whether that person is a minor or not)); (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses, which reveals whether a user is located in California). Bat.bing.com updates this information each time a user clicks on a website hosting a third-party bat.bing.com cookie. Bat.bing.com keeps this user data for six months.

87. Bat.bing.com cookies help Microsoft track users' interactions with ads (e.g., clicking a link or making a purchase) and provide valuable metrics that advertisers use to measure ad campaign performance. Further, bat.bing.com cookies allow Microsoft to obtain and store at user data to "help [website owners] focus a campaign or ad group on potential audiences who meet [website owners'] specific criteria, so [website owners] can increase the chance that [consumers] see [website owners'] ads."[32] Further, bat.bing.com offers [website owners] valuable "conversion tracking," which is a "measure [of] the ROI (return on investment) of your advertising campaign by letting [website owners] assign a monetary value to the activities people complete on [Defendant's] website after clicking [website owners'] ad."[33]

88. Microsoft also utilizes bat.bing.com data for its own purposes, including by using the data to tailor content and target advertisements to users. This profile enables Microsoft to deliver highly targeted ads within Microsoft's extensive advertising network Microsoft's revenue from its advertising network program has exceeded $10 billion as of 2022.[34]

[29] https://help.ads.microsoft.com/#apex/ads/en/60212/0.
[30] *Id.*
[31] *Id.*
[32] https://help.ads.microsoft.com/#apex/ads/en/60212/0.
[33] https://help.ads.microsoft.com/#apex/ads/en/56680/2.
[34] https://digiday.com/media/microsofts-ad-revenue-hit-10b-and-its-investing-is-a-sleeping-giant-about-to-wake/.

6. Adobe Cookies.

89. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices, even after users adjust the "Do not sell my personal information" toggle switch to reject cookies, to and from the **demdex.net** domain. This domain is associated with Adobe Inc.'s Audience Manager, a data management platform, Adobe's Marketing Cloud, and Adobe's Experience Cloud Identity Service, a service which provides a universal, persistent ID to identify visitors across all Adobe products.

90. Adobe cookies are used to assign a unique identifier to each site visitor, which enables Adobe to consistently recognize and track users across different sessions and domains (i.e., cross-site tracking) and collect and synchronize user data to comprehensively observe and evaluate user behavior online.[35] These cookies enable Adobe to obtain and store at least the following user data: (i) user identifier; (ii) website interactions; (iii) browsing history; (iv) visit history; (v) interests and preferences; and (vi) session information.[36]

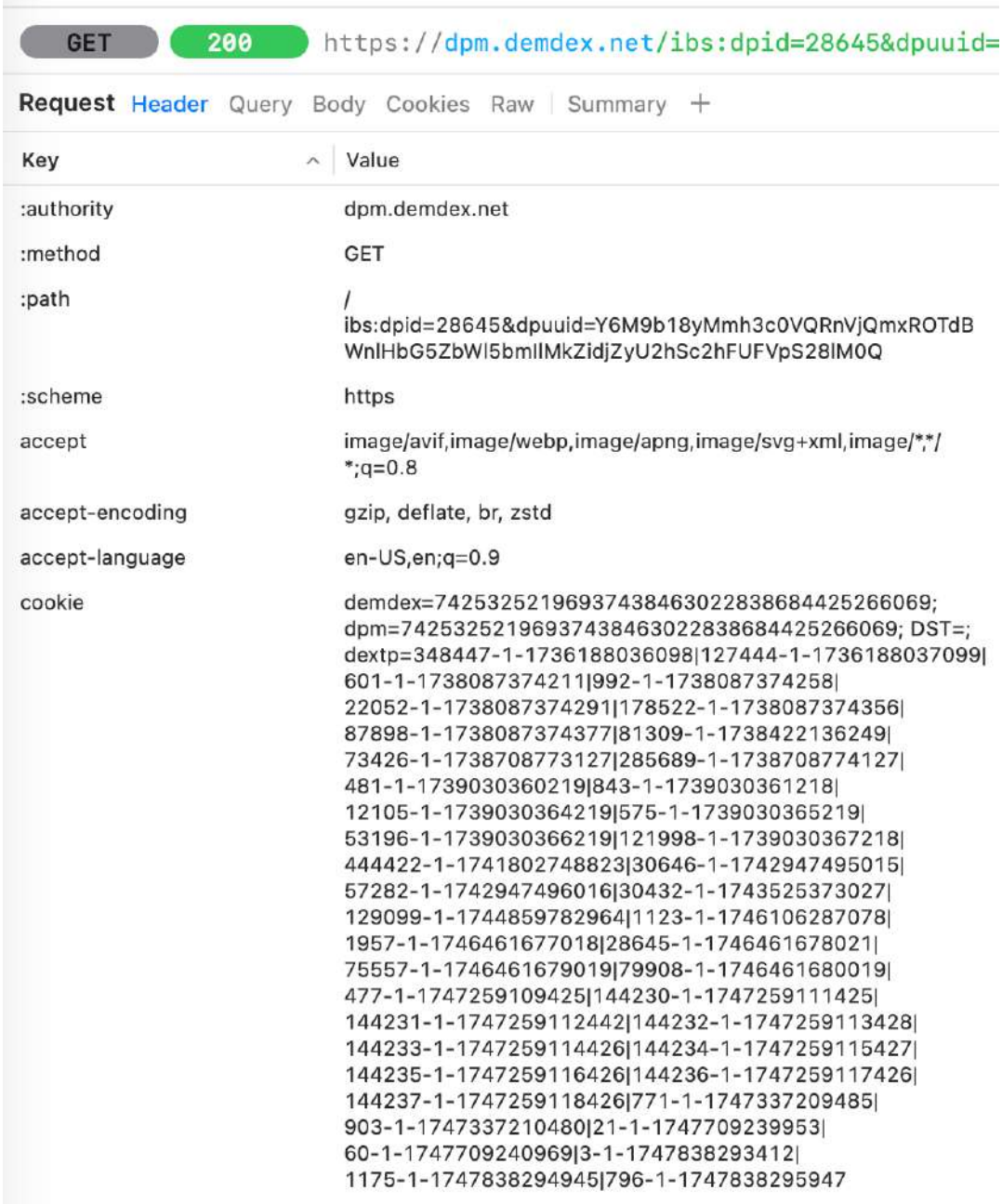
91. Adobe aggregates this cookie data with other data from multiple channels and devices, including web analytics, CRM systems, and e-commerce platforms, to create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics, create audience segments based on shared traits (such as Millennials, Californians, tech enthusiasts, etc.), and to enable targeted advertising and marketing analytics.[37]

[35] *See, e.g.,* Adobe Experience League: Adobe Analytics cookies (available at https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/analytics); *see also* Adobe Experience League: Audience Manager cookies (available at https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager).

[36] *See, e.g.,* Adobe Audience Manager User Guide: Data Collection Components (available at https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/system-components/components-data-collection).

[37] *See, e.g.*, Adobe Audience Manager User Guide: Understanding Calls to the Demdex Domain (available at https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/demdex-calls); Adobe Experience Cloud Identity Service overview (available at https://experienceleague.adobe.com/en/docs/id-service/using/intro/overview); Adobe Audience Manager Features (available at https://business.adobe.com/products/audience-manager/features.html); *see also* Audience Manager Overview (available at https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/overview/aam-overview).

92. For example, the Adobe software code that Defendant causes to be stored on and executed by the Website user's device causes the following data to be sent to Adobe's domain, at dpm.demdex.net:

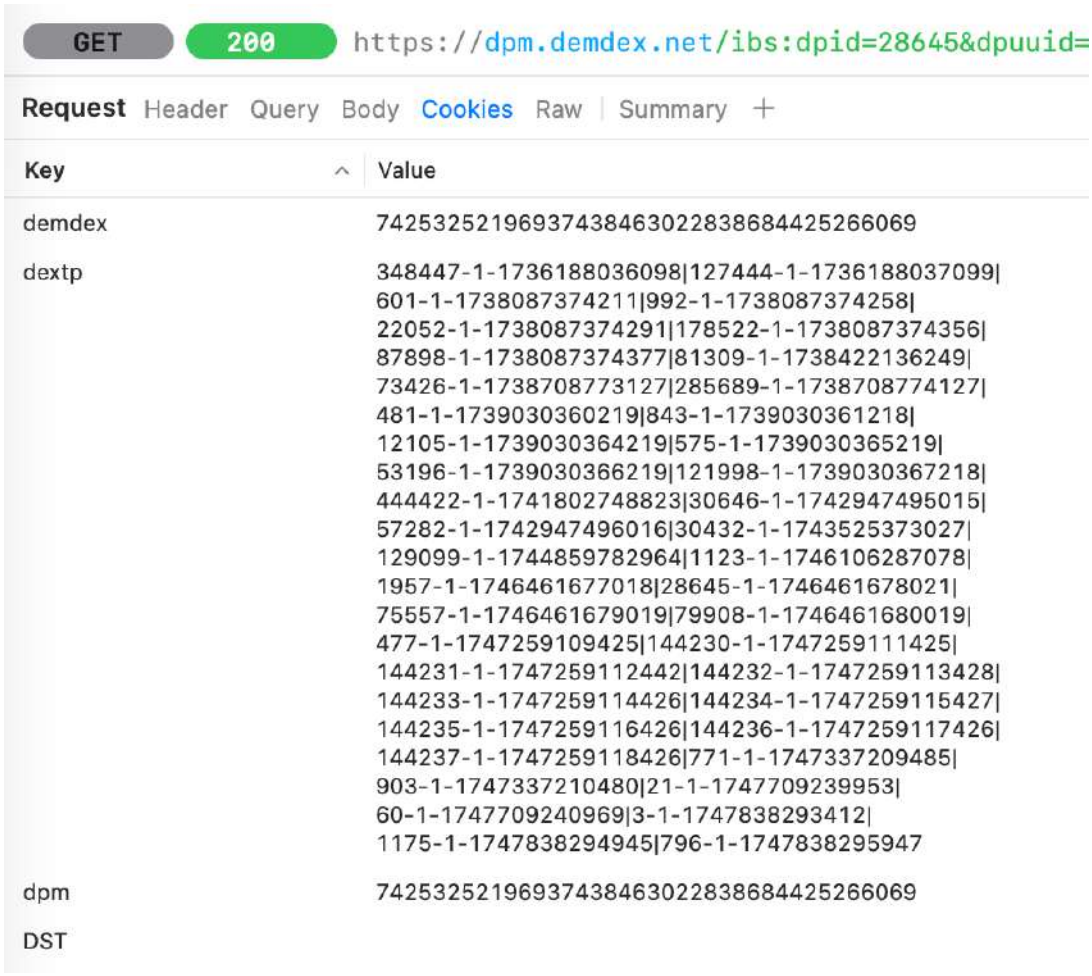


GET 200 https://dpm.demdex.net/ibs:dpid=28645&dpuuid=

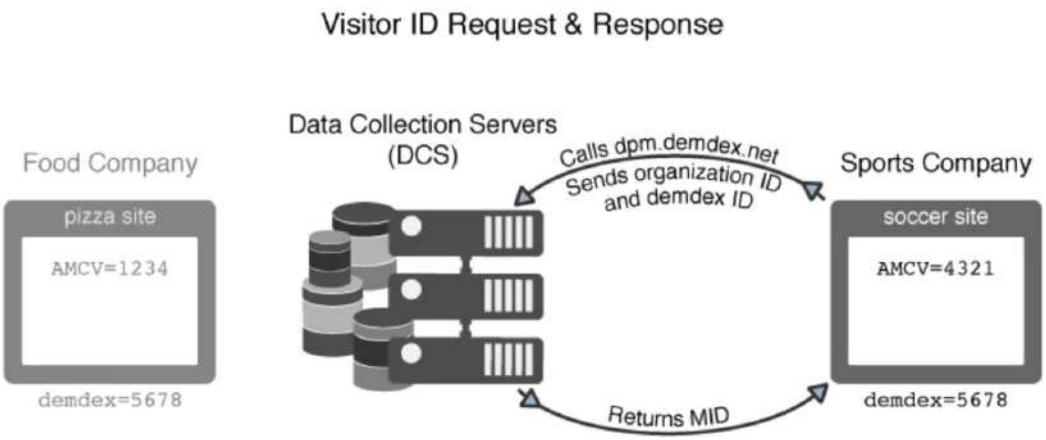
Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	dpm.demdex.net
:method	GET
:path	/ ibs:dpid=28645&dpuuid=Y6M9b18yMmh3c0VQRnVjQmxROTdB WnlHbG5ZbWl5bmlIMkZidjZyU2hSc2hFUFVpS28lM0Q
:scheme	https
accept	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/ *;q=0.8
accept-encoding	gzip, deflate, br, zstd
accept-language	en-US,en;q=0.9
cookie	demdex=74253252196937438463022838684425266069; dpm=74253252196937438463022838684425266069; DST=; dextp=348447-1-1736188036098|127444-1-1736188037099| 601-1-1738087374211|992-1-1738087374258| 22052-1-1738087374291|178522-1-1738087374356| 87898-1-1738087374377|81309-1-1738422136249| 73426-1-1738708773127|285689-1-1738708774127| 481-1-1739030360219|843-1-1739030361218| 12105-1-1739030364219|575-1-1739030365219| 53196-1-1739030366219|121998-1-1739030367218| 444422-1-1741802748823|30646-1-1742947495015| 57282-1-1742947496016|30432-1-1743525373027| 129099-1-1744859782964|1123-1-1746106287078| 1957-1-1746461677018|28645-1-1746461678021| 75557-1-1746461679019|79908-1-1746461680019| 477-1-1747259109425|144230-1-1747259111425| 144231-1-1747259112442|144232-1-1747259113428| 144233-1-1747259114426|144234-1-1747259115427| 144235-1-1747259116426|144236-1-1747259117426| 144237-1-1747259118426|771-1-1747337209485| 903-1-1747337210480|21-1-1747709239953| 60-1-1747709240969|3-1-1747838293412| 1175-1-1747838294945|796-1-1747838295947

dnt	1
Host	dpm.demdex.net
priority	i
sec-ch-ua	"Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"



93. In addition to receiving the referer and user-agent headers, Adobe receives the user's IP address and the "demdex" cookie. The "demdex" cookie contains a unique user ID, enabling Adobe to identify the user browsing the Website, and to track that user across multiple domains. Adobe's documentation depicts this as follows:



(*See* https://experienceleague.adobe.com/en/docs/id-service/using/intro/id-request.)

7. Taboola Cookies.

94. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices, even after users adjust the "Do not sell my personal information" toggle switch, to and from the **taboola.com** domain.[38] This domain is associated with Taboola, Inc., "one of the world's leading performance advertising platforms for the open web. Through our exclusive partnerships with many of the world's top websites, we help advertisers engage with over 600 million unique daily active users."[39] "Taboola's platform is powered by Deep Learning technology that uses Taboola's unique data about people's interests and information consumption to recommend the right content to the right person at the right time."[40] Taboola's technology learns user engagement patterns by analyzing data it collects using cookies about user "reading preferences, browsing history, device, location, time of day and more..."[41]

95. Taboola cookies enable it to obtain and store at least the following user data: user identifiers, browsing history, visit history, website interactions, user input data (such as email addresses), demographic information (such as gender and age), interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers

[38] *See* LiveRamp Product and Service Privacy Notice (available at https://liveramp.com/privacy/service-privacy-policy/).
[39] See https://help.taboola.com/hc/en-us/articles/115006597307-How-Taboola-Works#.
[40] *Id.*
[41] *Id.*

(i.e., "cookie IDs"), and/or geolocation data, including whether a user is located in California.[42] This data allows Defendant to target its advertising campaigns to users based on user "location, time, browser type, connection type, audience segments, and more."[43]

96. Defendant specifically identified Taboola as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

97. For example, the Taboola software code that Defendant causes to be stored on and executed by the Websites user's device causes the following data to be sent to Taboola's domain, at sync-t1.taboola.com:

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

[42] Taboola Privacy Policy (available at https://www.taboola.com/policies/privacy-policy#information-we-collect-from-users-user-information); *see also* Taboola Cookie Policy (available at https://www.taboola.com/policies/cookie-policy).

[43] *See* https://help.taboola.com/hc/en-us/articles/115006597307-How-Taboola-Works#; *see also* https://help.taboola.com/hc/en-us/articles/115001936293-Targeting-Marketplace-Audiences#.

GET 200 https://sync-t1.taboola.com/sg/criteortb-networ

Request Header Query Body Cookies Raw Summary +

Key	Value
:authority	sync-t1.taboola.com
:method	GET
:path	/sg/criteortb-network/1/rtb-h/?taboola_hm=k-z7KSz3g_4xbh7mQXaizc36ula0AbB-nzjquGFA
:scheme	https
accept	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding	gzip, deflate, br, zstd
accept-language	en-US,en;q=0.9
cookie	t_gid=79fcfbc0-0af5-4f13-8e3e-491a6d918b01-tucte71ffd8; taboola_vmp=temurtbnative-network
dnt	1
Host	sync-t1.taboola.com
priority	i
sec-ch-ua	"Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
sec-fetch-dest	image
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
sec-fetch-storage-access	active
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36

GET 200 https://sync-t1.taboola.com/sg/criteortb-networ

Request Header Query Body Cookies Raw Summary +

Key	Value
taboola_hm	k-z7KSz3g_4xbh7mQXaizc36ula0AbB-nzjquGFA

GET 200 https://sync-t1.taboola.com/sg/criteortb-networ

Request Header Query Body Cookies Raw Summary +

Key	Value
t_gid	79fcfbc0-0af5-4f13-8e3e-491a6d918b01-tucte71ffd8
taboola_vmp	temurtbnative-network

98. According to Taboola documentation, the "t_gid" cookie belongs to the category of "[a]dvertising cookies used for user identification and targeted advertising."[44]

99. Taboola explains in its Privacy Policy the user data it receives from cookies installed on its customers' (such as Defendant) websites and how it uses (and monetizes) that data to create audience segments as follows:

> We use User Information for the following purposes: … **Offering our Customers data segments that help target content and advertisements for topics, products, and services that may interest you.** A data segment is a grouping of users who share one or more attributes (e.g., travel enthusiasts). We offer a number of data segments, both proprietary and from our data partners, to our Customers so that they may better target Users who are more likely to be interested in their content and advertisements. Taboola does not knowingly create segments that are based upon what we consider to be sensitive information (for example, Personal Data revealing your racial or ethnic origin or your religious affiliations, or Personal Data concerning your sensitive health information, sex life or sexual orientation, or genetic or biometric data). In connection with our Services, our Customers may use these standard health-related segments about non-sensitive conditions such as an inferred interest in health and wellness or over the counter medications. In addition, Taboola offers our Customers standard political-related segments that may indicate general political sentiment, interest in specific political issues, and political party affiliation.[45]

8. LiveRamp Cookies.

100. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices, even after users adjust the "Do not sell my personal information" toggle switch to reject cookies, to and from the **liadm.com** domain.[46] This domain is associated with LiveRamp, a software company that allows businesses to combine customer data from various online and offline sources and leverage that data for marketing and analytics purposes.[47] Liadm.com cookies are used to create an online identification code for the purpose of recognizing users' devices and tracking their user behavior.

101. These cookies enable LiveRamp to obtain and store at least the following user data: browsing history, visit history, website interactions, user input data (such as email address),

[44] https://policies.taboola.com/cookie-policy/.
[45] Taboola Privacy Policy (available at https://www.taboola.com/policies/privacy-policy#information-we-collect-from-users-user-information) (emphasis in original).
[46] *See* LiveRamp Product and Service Privacy Notice (available at https://liveramp.com/privacy/service-privacy-policy/).
[47] See https://liveramp.com/privacy/service-privacy-policy/#section1a; *see also* LiveRamp Data Marketplace (available at https://liveramp.com/data-marketplace/).

demographic information, interests and preferences, device information, user identifiers, and geolocation data (including IP addresses, which can be used to determine whether a user is located in California), on the Website. The unique user identifier enables LiveRamp to sell a user's unique data for use in online and cross-channel advertising (including targeted advertising and email marketing).

102. LiveRamp explains in its Privacy Notice the user data it receives from cookies installed on "partner websites" and how it uses (and monetizes) that data as follows:

> [The website] partner may sell or share personal information collected from you, such as your email, cookies set on your browser, IP address, or information about your browser or operating system, with LiveRamp. LiveRamp uses this information to create an online identification code for the purpose of recognizing your device. This code may be placed in our partners' cookie and for use in online and cross-channel advertising (including targeted advertising and email marketing), or LiveRamp may connect it to LiveRamp's own 3rd-party cookie and other identifiers. In addition, by associating an email address with a cookie, LiveRamp and third parties can link your browsing activity across different websites and other applications and services to your specific device associated with the email address, identifying the user behind the device. This means that, even when browsing unrelated sites, your online activity can be connected to you for advertising and other marketing-related purposes, including email marketing and offline advertising...
>
> The personal data and identifiers we collect (for instance, a cookie ID) may be linked to other personal data and identifiers through known associations and/or identity resolution (for instance, an identifier derived from or associated with a hashed email address and LiveRamp cookie 1234 might be associated with partner cookie 5678), and shared with advertising partners and other third party advertising companies for the purpose of enabling interest-based content or targeted advertising throughout your online and offline experiences (e.g., web, TV [MVPDs], connected TV, mobile applications, email marketing and other media). These third parties may in turn use this identifier to link demographic or interest-based information you have provided in your interactions with them. Note that LiveRamp does not itself provide the service of targeted advertising (sometimes referred to as "cross-context advertising") but, rather, processes and transfers data to an advertiser's advertising platform so that platform can provide targeted advertising services...[48]

9. Additional Third-Party Cookies.

103. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices, even after users adjust the "Do not sell my personal information" toggle switch to reject cookies, to and from other domains, including (i) pubmatic.com, (ii)

[48] *Id.*

ib.adnxs.com, (iii) rubiconproject.com, (iv) criteo.com, (v) casalemedia.com, (vi) bidswitch.net, (vii) amazon-adsystem.com, (viii) pinterest.com, (ix) reddit.com, (x) 3lift.com, (xi) match.adsrvr.org, (xii) tr.snapchat.com, and (xiii) teads.tv.

104. The **pubmatic.com** domain is associated with PubMatic, Inc., a digital advertising company.[49] PubMatic uses pubmatic.com cookies to collect data on user behavior on websites including user interactions with advertising content.[50] PubMatic uses this data to personalize advertising content and track users across the internet.[51]

105. Defendant specifically identified PubMatic as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

106. The **adnxs.com** domain is associated with AppNexus, owned by Microsoft. Microsoft uses adnxs.com cookies to collect data on user navigation and behavior on websites, including information on user preferences and/or interaction with web-campaign content, to target advertisements.[52] The cookies include unique identifiers that help Microsoft recognize users across different websites and sessions.[53] This allows cookies set from the adnxs.com domain to collect data, including IP address, user demographic information, geographic location, page views, and interactions with websites.[54] These cookies also enable Household Attribution, a feature that enables Microsoft to match ads served on any device to website activity occurring on any device connected to the same network using the same IP address.[55] Further, the cookies enable advertisers to track the effectiveness of campaigns and avoid showing the same ads repeatedly to the same users. Microsoft uses this data to personalize ad content and track users across the internet. Adnxs.com cookies also categorize users into different segments based on

[49] *See* www.metrixlab.com.
[50] *See*, PubMatic, Inc. Form 10-K for year ending December 31, 2023 (Filed February 28, 2024) at 17–18.
[51] *Id*.
[52] https://cookiepedia.co.uk/host/adnxs.com.
[53] https://learn.microsoft.com/pdf?url=https%3A%2F%2Flearn.microsoft.com%2Fen-us%2Fxandr%2Fmonetize%2Ftoc.json.
[54] *Id*.; https://www.microsoft.com/en-us/privacy/privacystatement#mainpersonaldatawecollectmodule.
[55] https://learn.microsoft.com/pdf?url=https%3A%2F%2Flearn.microsoft.com%2Fen-us%2Fxandr%2Fmonetize%2Ftoc.json.

their interests, demographics, or behaviors. This segmentation is used to target specific audiences with tailored ads. The data collected by cookies set through the adnxs.com domain has allowed Microsoft to set up a platform in which advertisers can bid for and place advertisements targeted at users based on a variety of demographics, including, among other things, demography, device type, and location.[56]

107. Defendant specifically identified Microsoft as a provider of "Marketing and Advertising" and "Performance & Analytics" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

108. The **rubiconproject.com** domain is associated with the Rubicon Project, an advertising exchange platform owned by Magnite, Inc.[57] Rubicon Project operates as a Supply-Side Platform (SSP), enabling website publishers to sell their advertising inventory through real-time bidding auctions. Its cookies are used to assign unique identifiers to users, collect data on their browsing behavior (including IP address, location, and websites visited), and facilitate the exchange of this user data with various ad services.[58] This process, known as cookie syncing, allows advertisers to identify and bid on ad impressions to target specific users across the web, forming a foundational component of the programmatic advertising ecosystem.[59]

109. Defendant specifically identified Rubicon Project as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

110. The **criteo.com** domain is associated with Criteo S.A., a digital advertising company that provides online advertisements.[60] Criteo S.A. uses cookies set with the criteo.com domain to build a unique profile for each website user and to target those users with advertisements.[61] Cookies set with the Criteo.com domain assign a unique identifier to users'

[56] https://learn.microsoft.com/en-us/xandr/monetize/buy-side-targeting#other-targeting-guidance.
[57] *See* Platform Cookie Policy - Magnite, accessed September 26, 2025, https://www.magnite.com/legal/platform-cookie-policy/.
[58] *See id.*; *See also* User Choice Portal | Manage Your Privacy Preferences with Magnite, accessed September 26, 2025, https://www.magnite.com/legal/user-choice-portal/.
[59] *See id.*
[60] *See* https://www.criteo.com/platform/commerce-media-platform/.
[61] https://www.criteo.com/advertising-guidelines/.

browsers and devices, and collect data on user's pages views, behavior on websites, information on user preferences and/or interaction with advertisements, and products users have viewed, put in their digital shopping carts, and/or purchased.[62] Criteo S.A. uses this data to personalize ad content and track users across the internet to, among other things, target, price, place, and schedule advertisements.[63]

111. Defendant specifically identified Criteo as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

112. The **casalemedia.com** domain is associated with Casale Media, a digital advertising technology company that operates as part of an ad exchange network.[64] Casale Media's cookies are used to collect data about users' website visits and online behavior, including the number of visits, time spent on sites, and pages loaded.[65] This information is used to build user profiles for the purpose of delivering targeted advertising.[66] The platform enables advertisers to segment audiences and optimize ad relevance by tracking users across multiple websites within its network, and its cookies can also be used for functions like frequency capping to limit the number of times a user is shown the same advertisement.[67]

113. Defendant specifically identified Index Exchange as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

114. The **bidswitch.net** domain is associated with BidSwitch, a technology platform owned by IPONWEB GmbH that functions as middleware in the programmatic advertising ecosystem.[68] BidSwitch's cookies are not used to directly serve ads to users, but rather to facilitate the service of ads between Supply-Side Platforms (SSPs) and Demand-Side Platforms

[62] *Id.*; https://cookiepedia.co.uk/cookies/criteo.
[63] *Id.*
[64] *See* https://www.indexexchange.com/about/.
[65] *See* https://www.indexexchange.com/privacy/exchange-platform-privacy-policy/.
[66] *Id.*
[67] *Id.*
[68] *See* https://www.bidswitch.com/.

(DSPs).[69] The cookies store unique user IDs and regulate the synchronization of these IDs across different advertising services.[70] This "cookie syncing" is essential for enabling advertisers on various platforms to recognize a user and participate in real-time bidding auctions for ad space on publisher websites, effectively acting as a central hub for identity matching in the ad-tech industry.[71]

115. Defendant specifically identified Bidswitch as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

116. The **amazon-adsystem.com** domain is associated with Amazon's advertising services. Amazon utilizes cookies to collect data on user interactions with websites (including browsing behavior and preferences) to perform advertising and personalization functions, i.e., to assist Amazon in delivering advertisements tailored to user interests. Further, the cookies perform analytics functions to enable Amazon to measure and analyze the performance of its services and to ensure that ads are effective and relevant.

117. Defendant specifically identified Amazon as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

118. The **pinterest.com** domain is associated with Pinterest, Inc., a popular social media platform that allows users to discover, save, and share ideas as pins in the form of photos and videos. Businesses can upload and showcase their products through "Shop the Look" pins or Product Pins that directly link to e-commerce websites. Businesses install the Pinterest tag on their websites to track ad conversions. As Pinterest explains, "The Pinterest tag is a piece of code that you add to your website. It lets Pinterest track visitors to your site, as well as the actions they take on your site after seeing your Pinterest ad. This means you can measure how effective your Pinterest ads are by understanding the actions people take on your website after seeing or

[69] *See* https://www.bidswitch.com/privacy-policy/.
[70] *Id.*
[71] https://clearcode.cc/blog/what-is-bidswitch/.

engaging with your ad."[72] Pinterest cookies can be used to identify and track people who purchase products, add items to a shopping cart, visit specific pages on the website, and/or search for specific items on the website.[73]

119. Defendant specifically identified Pinterest as a provider of "Performance & Analytics" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

120. The **reddit.com** domain is owned by Reddit, Inc., a popular online platform where users connect over shared interests, participate in discussions, and learn about what's relevant in the world."[74] Businesses can leverage the platform for marketing and advertising businesses to "build brand awareness, drive purchase consideration for [ ] products, and drive sales by engaging in subreddit conversations, sharing valuable (or even exclusive) content, and using Reddit Ads."[75] Reddit cookies and tracking technologies allow businesses to "track redditors who have interacted with your website and to craft personalized ads to keep them engaged."[76] Reddit cookies can be used to identify and target advertisements to users based on "previous clicks, likes, or comments, you nurture leads and guide them toward making a purchase or taking another desired action."[77] Further, using Reddit's audience targeting features allow businesses to "reach users based on their interests and passions in the places where they're most engaged" and target audience segments based on gender, location, interests, devices, and more.[78]

[72] Pinterest Help Center: Install the Pinterest Tag (available at https://help.pinterest.com/en/business/article/install-the-pinterest-tag).
[73] *See, e.g.*, Pinterest Help Center: Add event codes (available at https://help.pinterest.com/en/business/article/add-event-codes); Pinterest Help Center: View tag parameters and cookies (available at https://help.pinterest.com/en/business/article/pinterest-tag-parameters-and-cookies).
[74] https://www.business.reddit.com/learn/what-is-reddit.
[75] *Id.*
[76] https://www.business.reddit.com/advertise/targeting.
[77] https://www.business.reddit.com/advertise/targeting/custom/.
[78] https://business.reddithelp.com/s/article/Overview-Reddit-Ads-Audience-and-Targeting; https://business.reddithelp.com/s/article/demographics#gender-targeting; https://business.reddithelp.com/s/article/demographics#location-targeting; https://business.reddithelp.com/s/article/reddit-audiences; and https://business.reddithelp.com/s/article/demographics.

121. Defendant specifically identified Reddit as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

122. The **3lift.com** domain is associated with TripleLift, Inc., an advertising technology platform that specializes in programmatic advertising.[79] TripleLift's cookies are used to assign a unique digital identifier (stored in the "TLUID" cookie) to a user's browser or device.[80] This identifier enables the tracking of users across different websites to collect data for targeted advertising, including interest-based targeting and ad performance measurement.[81] The company also leverages first-party publisher data to create audience segments, positioning this as an addition to traditional third-party cookie tracking in response to industry privacy changes.[82]

123. Defendant specifically identified TripleLift as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

124. The **match.adsrvr.org** domain is associated with The Trade Desk, Inc., a digital advertising company that offers a cloud-based ad-buying platform that enables businesses to plan, manage, optimize, and measure data-driven digital advertising campaigns.[83] The Trade Desk uses insight.adsrvr.org cookies to collect data on users such as their geographic locations, the type of device users are using, and users' interests as inferred from their web browsing or app usage activity."[84] This data helps The Trade Desk personalize ad content and track users across the internet.[85]

125. The Trade Desk acknowledges that its cookies' ability "to collect, augment, analyze, use and share data relies upon the ability to uniquely identify devices across websites

[79] *See* https://triplelift.com/.
[80] *See* https://triplelift.com/user-rights-policy-and-opt-out/.
[81] *See* https://triplelift.com/platform-privacy-policy/.
[82] *See* https://triplelift.com/resources/case-study/triplelift-audiences-exceed-benchmarks/.
[83] *See* The Trade Desk, Inc. 2023 Form 10-K (filed February, 15 2024).
[84] *Id.*
[85] *Id.*

and applications, and to collect data about user interactions with those devices for purposes such as serving relevant ads and measuring the effectiveness of ads."[86]

126. Defendant specifically identified The Trade Desk as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

127. The **tr.snapchat.com** domain is associated with Snap Inc., the social media company that owns Snapchat. Snapchat is multimedia messaging app that lets users share photos, videos, text, and drawings—often designed to disappear after being viewed. Snapchat uses tr.snapchat.com cookies to collect data on browsing history, choices, and interactions with advertisements.[87] This data helps Snap personalize ad content and track users across the internet.[88] As Snap explains, it uses the data collected by Snapchat cookies "for optimization, custom audience creation, look-alike modeling, reporting, machine learning, and targeting capabilities. All uses are … meant to deliver better results for our ad products."[89]

128. Defendant specifically identified SnapChat as a provider of "Marketing and Advertising" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

129. The **teads.tv** domain is associated with Teads SA, which operates a "Global Media Platform" that seeks to provide advertisers with audience information across media, including websites and television.[90] Accordingly, Teads utilizes both cookies and other tracking technologies to collect data on user interactions with websites (including browsing behavior and preferences) to perform advertising and personalization functions, i.e., to assist Teads and its customers in delivering advertisements tailored to user interests. Further, the cookies perform

---

[86] *Id*.
[87] https://snapdiscoveries.com/what-is-tr-snapchat-com-is-used-for; *see also* Snapchat Business Help Center: Directly Implement the Pixel On Your Website (available at https://businesshelp.snapchat.com/s/article/pixel-direct-implementation).
[88] *Id*.
[89] Snapchat Business Help Center: Pixel Implementation FAQ (available at https://businesshelp.snapchat.com/s/article/snap-pixel-faq); *see also* Snapchat Business Help Center: About Snap Pixel (available at https://businesshelp.snapchat.com/s/article/snap-pixel-about).
[90] *See* Teads: The platform that means business (available at https://www.teads.com/).

analytics functions to enable Teads to measure and analyze the performance of its services and to ensure that ads are effective and relevant "across the marketing funnel" across websites,[91] such as Defendant's Website.

130. Defendant specifically identified Teads as a provider of "Functional" cookies that users could deny by adjusting the "Do not sell my personal information" toggle switch.

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

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

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

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

134. Second, the Third Parties read the data in real time in order to ***deduplicate*** events transmitted through multiple channels. Most websites transmit the same user interaction twice: both directly from the user's device and separately through a server-to-server API, to ensure

[91] *Id.*

reliability.[92] Third Party platforms encourage this redundant configuration and automatically compare identifiers contained within the transmitted data—such as event identifiers and device identifiers—to determine whether multiple transmissions correspond to the same user action.[93] This deduplication occurs as the communications are received, before they are stored.

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

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

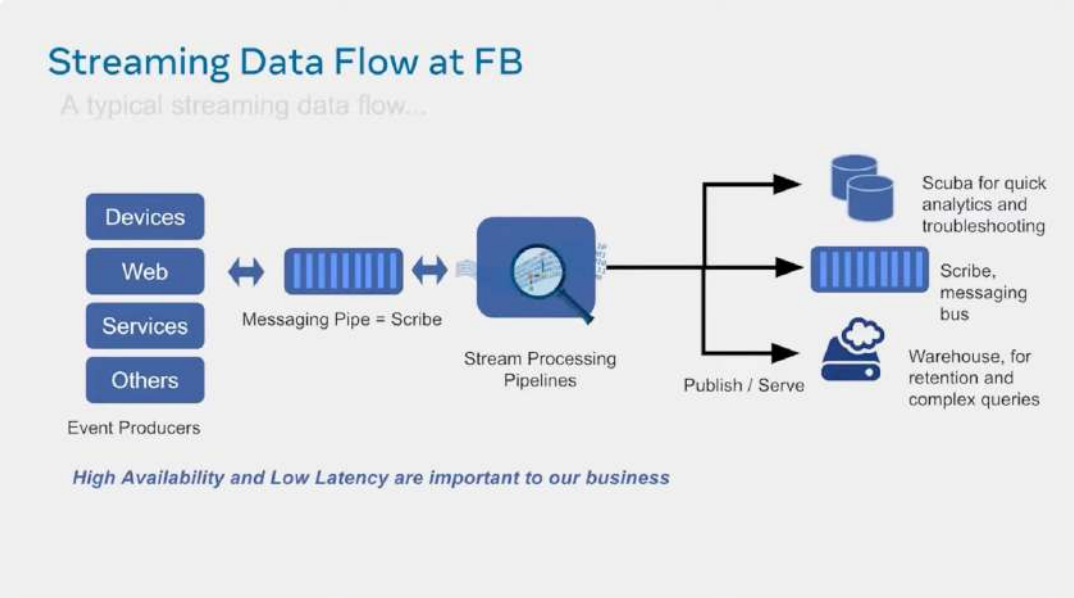
137. To accomplish each of the functions described above, the Third Parties employ real-time stream processing platforms specifically designed to operate on data "in flight"—that is, after it is transmitted from a user's browser but before it is committed to the Third Parties' storage. Examples of such platforms include Apache Flink, Kafka, and Amazon Kinesis.

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

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

Industry documentation confirms that these systems are designed to read, transform, analyze, and act upon data streams as they are received.

138. For example, Meta (formerly Facebook) has publicly described its proprietary real-time stream processing platform that ingests data transmitted from users' devices and websites, applies real-time transformations and personalization, and only thereafter stores the data in backend data warehouses, as illustrated in the following diagram created by Facebook:[94]



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

140. Facebook's Stream Processing Pipelines perform a wide variety of real-time analytics, transformations, and AI and machine learning on the data prior to storage:[95]

[94] XStream: Stream Processing Platform at Facebook (video) at 1:07 (available at https://www.youtube.com/watch?v=DNI54vc1ALQ).
[95] *Id.* at 2:05.

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

142. On information and belief, the other Third Parties also use ingest-phase processing platforms that perform real-time analytics and filtering on incoming data streams before storage. For example, Google developed MillWheel, an internal stream processing system, as well as Flume/FlumeJava, which evolved into Google Cloud Dataflow.[96] Google Cloud Dataflow enables Google to perform many functions on real-time data at the "Ingest" phase, before it is stored.[97] Google, which sells Dataflow to third party developers for use with their own products, states that Dataflow is used "to create data pipelines that read from one or more sources, ***transform the data***, and write the data to a destination."[98] One use for Dataflow

[96] *See, e.g.*, Google Cloud Blog, "How cloud batch and stream data processing works" (August 2020), https://cloud.google.com/blog/products/data-analytics/how-cloud-batch-and-stream-data-processing-works.
[97] Google Cloud Blog, "BigQuery explained: An overview of BigQuery's architecture" (September 2, 2020), https://cloud.google.com/blog/products/data-analytics/new-blog-series-bigquery-explained-overview.
[98] Google Cloud Documentation, "Dataflow overview," https://docs.cloud.google.com/dataflow/docs/overview (emphasis added).

is the "[r]eal-time machine learning (ML) analysis of streaming data."[99] Google confirms that Dataflow is "suitable for more advanced applications, such as real-time streaming analytics."[100]

143. Pinterest uses Apache Kafka, a third-party real-time stream processing platform.[101] The Kafka system streams events in real time to "many applications, such as native Kafka clients, Kafka Streams, Flink, and Spark streaming, which are consumers of a subset of Kafka topics that build several real-time pipelines."[102] These systems "include but are not limited to monetization, safety and spam detection, metrics processing, and experimentation use cases."[103]

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

E. The Signaling and Addressing Information Intercepted by the Third Parties.

122. The "signaling" and "addressing" information captured and recorded by the Third Parties includes TCP and/or UDP port numbers associated with outgoing communications initiated by Plaintiffs' and Class Members' browsers and devices. In the context of Internet Protocol (IP) networking, port numbers function as sub-addresses that direct traffic to specific software processes. By recording these port numbers, the Third Parties identify and distinguish specific network connections and the communicating endpoints involved (e.g., a Plaintiffs' or Class Member's IP address and TCP/UDP source port communicating with a Third Party's destination IP address and destination port such as 443). These port numbers constitute addressing information associated with the communications initiated by Plaintiffs' and Class

[99] *Id.*
[100] *Id.*
[101] Confluent, "Lessons Learned from Running Apache Kafka at Scale at Pinterest," https://www.confluent.io/blog/running-kafka-at-scale-at-pinterest/.
[102] *Id.*
[103] *Id.*

Members' browsers and devices and fall within the "instruments" and "facilities" contemplated by California Penal Code § 638.50(b).

123. The "signaling" information also includes protocol-level metadata recorded by the Third Parties during connection establishment and session management, such as the initiation and acceptance of TCP connections and the TLS handshake and negotiation metadata used to establish HTTPS sessions. This signaling information is transmitted by Plaintiffs' and Class Members' devices to initiate, coordinate, and manage electronic communications with the Third Parties. Because this metadata enables management of the connection rather than the substance of the message, it constitutes record information regarding the characteristics of the communication, rather than communication content, and falls squarely within the statutory definition of a pen register.

124. Additionally, the Third Parties record HTTP request header metadata, such as the "Host" header and connection-management headers (e.g., "Connection" in HTTP/1.1), which function as digital "dialing" information. Just as a traditional pen register records the number dialed to reach a destination, these headers identify the intended web origin (via "Host") and specify how the client requests the connection be handled for that request (e.g., whether to keep the connection open). This header information is transmitted as part of the Plaintiffs' and Website users' HTTP requests and, together with the destination network address and port, enables the receiving Third Party to identify and log the destination and handling characteristics of Plaintiffs' and Website users' communications, separate from any underlying user input or message content.

125. Finally, the Third Parties' receiving infrastructure (e.g., servers, edge services, and/or load balancers) observes and records network-level and transport-level routing and addressing metadata associated with communications initiated by Plaintiffs' and Website users' browsers and devices. This metadata includes destination IP addresses, port identifiers (such as 443 for HTTPS), and related connection and session attributes, including connection initiation and termination timestamps, connection duration, and identifiers such as the protocol used (TCP or UDP), the source IP address, the source port, the destination IP address, and the destination

port. The Third Parties use this information in real time to identify and log the origin and destination endpoints of Plaintiffs' and Website users' electronic communications and the characteristics of those connections, separate from any substantive "message" or "contents" carried at the higher-level Application layer.

F. The Private Communications Collected are Valuable.

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

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

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

129. The value of the Private Communications tracked and collected by the Third Parties using cookies on the Website can be quantified. Legal scholars observe that "[p]ersonal

information is an important currency in the new millennium."[104] Indeed, "[t]he monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend." *Id*. "Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information." *Id*.

130. Numerous empirical studies quantify the appropriate value measure for personal data. Generally, the value of personal data is measured as either the consumer's willingness to accept compensation to sell them data or the consumer's willingness to pay to protect their information.

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

PLAINTIFFS' EXPERIENCES

Plaintiff Ewart

132. Plaintiff Ewart visited the Website to seek and obtain information about Defendant's products, including its guitars or other musical instruments, while located in California, on one or more occasions during the last four years.

133. Plaintiff Ewart's visits to the Website were consistent with those of an ordinary user seeking information about Defendant's products. Plaintiff Ewart is not a consumer advocate, a "tester," or a compliance auditor who visited the Website to test or evaluate Defendant's privacy practices. During her visits, Plaintiff Ewart viewed information on specific products.

134. When Plaintiff Ewart visited the Website, the Website immediately detected that she was a visitor in California and presented her with Defendant's popup cookie consent banner, which provided the option to adjust the "Do not sell my personal information" toggle switch. Plaintiff Ewart viewed Defendant's representation on the popup cookie consent banner that,

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

"Fender Musical Instruments Corporation…want[s] you to know that we and our partners process information about you, your devices, and your online behavior using technologies such as cookies to provide, analyse, and improve our services; to personalise content or advertising on this and other sites, apps, or platforms and to provide social media features." Plaintiff Ewart also viewed Defendant's additional representation that, rather than choosing to "rock out and accept these cookies" by first selecting the "OK" button without making any further selection, users could instead adjust the "Do not sell my personal information" toggle switch to decline or reject cookies, including those used for personalized advertising, analytics, and social media, as well as all those cookies associated with the sale or sharing of users' personal information.

135. Accordingly, Plaintiff Ewart believed that adjusting the "Do not sell my personal information" toggle switch on the popup cookie consent banner found on the Website would allow her to opt out of, decline, and/or reject all such cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of personal information to third-party advertising networks, analytics services, and social media companies for the purposes of providing personalized advertising, analytics, and social media functions).

136. Consistent with these representations, Plaintiff Ewart then adjusted the "Do not sell my personal information" toggle switch, and, only after adjusting this toggle, did she then click the "OK" button to confirm her choice. In rejecting the sale of her personal information, Plaintiff Ewart gave Defendant notice that she did not consent to the use or placement of cookies and tracking technologies that shared her information with third parties while browsing the Website. Further, Plaintiff Ewart specifically rejected, based on Defendant's representations, those cookies used to provide personalized advertising, analytics, and social media functions, and sell or share information with third parties for those and other purposes. In reliance on these representations and promises, only then did Plaintiff Ewart continue browsing the Website.

137. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused cookies and tracking technologies, including those used for personalized advertising, analytics, and social media, to be placed on Plaintiff Ewart's device and/or transmitted to the Third Parties along with user data, without Plaintiff Ewart's knowledge.

Accordingly, the popup cookie consent banner's representation to Plaintiff Ewart that she could reject the sale of her personal information, including the use and/or placement of all cookies and tracking technologies associated with such sales, or at least all personalized advertising, analytics, and social media cookies, while she browsed the Website was false. Contrary to what Defendant made Plaintiff Ewart believe, she did not have a choice about whether third-party cookies would be placed on her device and/or transmitted to the Third Parties along with her user data; rather, Defendant had already caused that to happen.

138. Then, as Plaintiff Ewart continued to browse the Website in reliance on the promises Defendant made in the popup cookie consent banner, and despite Plaintiff Ewart's clear rejection of the use and/or placement of all such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of cookies along with user data, including those involved in providing personalized advertising, analytics, and social media from the Third Parties, on her device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Ewart's Private Communications as Plaintiff Ewart browsed the Website.

139. Defendant's representations that consumers could decline or reject the sale of their personal information, including all third-party personalized advertising, analytics, and social media cookies, while Plaintiff Ewart and users browsed the Website were untrue. Had Plaintiff Ewart known this fact, she would not have used the Website. Moreover, Plaintiff Ewart reviewed the popup cookie consent banner prior to using the Website. Had Defendant disclosed that it would continue to cause cookies and tracking technologies to be stored on consumers' devices even after they choose to decline or reject all such cookies, Plaintiff Ewart would have noticed it and would not have used the Website or, at a minimum, she would have interacted with the Website differently.

140. Plaintiff Ewart continues to desire to browse content featured on the Website. Plaintiff Ewart would like to browse websites that do not misrepresent that users can decline or reject cookies and tracking technologies, including at least those personalized advertising, analytics, and social media cookies associated with the sale of users' personal information. If the Website were programmed to honor users' requests to decline or reject all such cookies and

tracking technologies, including at least those personalized advertising, analytics, and social media cookies that cause the sale or sharing of users' personal information, Plaintiff Ewart would likely browse the Website again in the future, but will not do so until then. Plaintiff Ewart regularly visits websites that feature content similar to that of the Website. Because Plaintiff Ewart does not know how the Website is programmed, which can change over time, and because she does not have the technical knowledge necessary to test whether the Website honors users' requests to decline or reject cookies and tracking technologies, Plaintiff Ewart will be unable to rely on Defendant's representations when browsing the Website in the future absent an injunction that prohibits Defendant from making misrepresentations on the Website. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Ewart is not a software developer and has not received training with respect to HTTP network calls.

Plaintiff Johnston

141. Plaintiff Johnston visited the Website to seek and obtain information about Defendant's products, including its guitars or other musical instruments, while located in California, on one or more occasions during the last four years including but not limited to, on or about April 28, 2025, April 29, 2025, May 3, 2025, and May 10, 2025. In particular, Plaintiff Johnston visited the Website to review product offerings, promotions, and spring sales, research specific musical instruments and amplifiers, including the Fender Princeton Reverb amplifier, and obtain information regarding products associated with the Guild brand. Plaintiff Ewart navigated the Website both by browsing product categories and webpages and by entering search terms into the Website's search tools.

142. Plaintiff Johnston's visits to the Website were consistent with those of an ordinary user seeking information about Defendant's products. Plaintiff Johnston is not a consumer advocate, a "tester," or a compliance auditor who visited the Website to test or evaluate

Defendant's privacy practices. During her visits, Plaintiff Johnston viewed information on specific products.

143. When Plaintiff Johnston visited the Website, the Website immediately detected that she was a visitor in California and presented her with Defendant's popup cookie consent banner, which provided the option to adjust the "Do not sell my personal information" toggle switch. Plaintiff Johnston viewed Defendant's representation on the popup cookie consent banner that, "Fender Musical Instruments Corporation…want[s] you to know that we and our partners process information about you, your devices, and your online behavior using technologies such as cookies to provide, analyse, and improve our services; to personalise content or advertising on this and other sites, apps, or platforms and to provide social media features." Plaintiff Johnston also viewed Defendant's additional representation that, rather than choosing to "rock out and accept these cookies" by first selecting the "OK" button without making any further selection, users could instead adjust the "Do not sell my personal information" toggle switch to decline or reject cookies, including those used for personalized advertising, analytics, and social media, as well as all those cookies associated with the sale or sharing of users' personal information.

144. Accordingly, Plaintiff Johnston believed that adjusting the "Do not sell my personal information" toggle switch on the popup cookie consent banner found on the Website would allow her to opt out of, decline, and/or reject all such cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of personal information to third-party advertising networks, analytics services, and social media companies for the purposes of providing personalized advertising, analytics, and social media functions).

145. Consistent with these representations, Plaintiff Johnston then adjusted the "Do not sell my personal information" toggle switch, and, only after adjusting this toggle, did she then click the "OK" button to confirm her choice. In rejecting the sale of her personal information, Plaintiff Johnston gave Defendant notice that she did not consent to the use or placement of cookies and tracking technologies that shared her information with third parties while browsing the Website. Further, Plaintiff Johnston specifically rejected, based on

Defendant's representations, those cookies used to provide personalized advertising, analytics, and social media functions, and sell or share information with third parties for those and other purposes. In reliance on these representations and promises, only then did Plaintiff Johnston continue browsing the Website.

146. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused cookies and tracking technologies, including those used for personalized advertising, analytics, and social media, to be placed on Plaintiff Johnston's device and/or transmitted to the Third Parties along with user data, without Plaintiff Johnston's knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Johnston that she could reject the sale of her personal information, including the use and/or placement of all cookies and tracking technologies associated with such sales, or at least all personalized advertising, analytics, and social media cookies, while she browsed the Website was false. Contrary to what Defendant made Plaintiff Johnston believe, she did not have a choice about whether third-party cookies would be placed on her device and/or transmitted to the Third Parties along with her user data; rather, Defendant had already caused that to happen.

147. Then, as Plaintiff Johnston continued to browse the Website in reliance on the promises Defendant made in the popup cookie consent banner, and despite Plaintiff Johnston's clear rejection of the use and/or placement of all such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of cookies along with user data, including those involved in providing personalized advertising, analytics, and social media from the Third Parties, on her device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Johnston's Private Communications as Plaintiff Johnston browsed the Website.

148. Defendant's representations that consumers could decline or reject the sale of their personal information, including all third-party personalized advertising, analytics, and social media cookies, while Plaintiff Johnston and users browsed the Website were untrue. Had Plaintiff Johnston known this fact, she would not have used the Website. Moreover, Plaintiff Johnston reviewed the popup cookie consent banner prior to using the Website. Had Defendant

disclosed that it would continue to cause cookies and tracking technologies to be stored on consumers' devices even after they choose to decline or reject all such cookies, Plaintiff Johnston would have noticed it and would not have used the Website or, at a minimum, she would have interacted with the Website differently.

149. Plaintiff Johnston continues to desire to browse content featured on the Website. Plaintiff Johnston would like to browse websites that do not misrepresent that users can decline or reject cookies and tracking technologies, including at least those personalized advertising, analytics, and social media cookies associated with the sale of users' personal information. If the Website were programmed to honor users' requests to decline or reject all such cookies and tracking technologies, including at least those personalized advertising, analytics, and social media cookies that cause the sale or sharing of users' personal information, Plaintiff Johnston would likely browse the Website again in the future, but will not do so until then. Plaintiff Johnston regularly visits websites that feature content similar to that of the Website. Because Plaintiff Johnston does not know how the Website is programmed, which can change over time, and because she does not have the technical knowledge necessary to test whether the Website honors users' requests to decline or reject cookies and tracking technologies, Plaintiff Johnston will be unable to rely on Defendant's representations when browsing the Website in the future absent an injunction that prohibits Defendant from making misrepresentations on the Website. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Johnston is not a software developer and has not received training with respect to HTTP network calls.

CLASS ALLEGATIONS

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

persons, defined as follows:

> **Class**: All persons who browsed the Website in the United States after declining or rejecting cookies by adjusting the "Do not sell my personal information" toggle switch on the Website's popup cookie consent banner.

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

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

153. **Common Questions Predominate:** This action involves common questions of law and fact to the Class because each class member's claim derives from the same unlawful conduct that led them to believe that Defendant would not cause third-party cookies to be placed on their browsers and devices and/or transmitted to third parties along with user data, after Class members chose to decline or reject cookies and tracking technologies on the Website, or at least those personalized advertising, analytics, and social media cookies responsible for selling or sharing users' personal information, nor would Defendant permit third parties to track and collect Class members' Private Communications as Class members browsed the Website.

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

a. Whether Defendant's actions violate California laws invoked herein; and

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

155. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, Plaintiffs, like the other Class members, visited the Website, declined or rejected cookies, and had her confidential Private Communications

intercepted by the Third Parties.

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

157. **Superiority:** There is no plain, speedy, or adequate remedy other than by maintenance of this class action. The prosecution of individual remedies by members of the Class will tend to establish inconsistent standards of conduct for Defendant and result in the impairment of Class members' rights and the disposition of their interests through actions to which they were not parties. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. Furthermore, as the damages suffered by each individual member of the Class may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

First Cause of Action: Invasion of Privacy

158. Plaintiffs reallege and incorporate the paragraphs of this Complaint as if set forth

herein.

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

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

161. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as Defendant affirmatively promised users they could opt out of, decline, or otherwise reject the sale of their personal information, and all third party cookies involved with that sale, including at least all personalized advertising, analytics, and social media cookies, by adjusting the toggle switch to do so, before proceeding to browse the Website. Plaintiffs and other Class members directed their electronic devices to access the Website and, when presented with the popup cookies consent banner on the Website, Plaintiffs and Class members declined or rejected cookies and reasonably expected that their declination or rejection of cookies and tracking technologies would be honored. That is, they reasonably believed that Defendant would not permit the Third Parties to store and send cookies and/or use other such tracking technologies on their devices while they browsed the Website. Plaintiffs and Class members also reasonably expected that, if they declined or rejected such cookies and/or tracking technologies, Defendant would not permit the Third Parties to track and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, on the Website.

162. Such information is "personal information" under California law, which defines

personal information as including "Internet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

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

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

165. Defendant's intrusion into Plaintiffs' privacy was also highly offensive to a reasonable person.

166. Defendant lacked a legitimate business interest in causing the placement and/or transmission of third-party cookies along with user data that allowed the Third Parties to track, intercept, receive, and collect Private Communications, including their browsing history, visit

history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, without their consent.

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

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

169. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' declination or rejection of the Website's use of cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Second Cause of Action: Intrusion Upon Seclusion

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

171. To assert a claim for intrusion upon seclusion, Plaintiffs must plead (i) that Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs have a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable person.

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

invited, welcomed, or authorized.

173. The Third Parties' tracking and collecting of Plaintiffs' and Class member's Private Communications on the Website using third-party cookies that Defendant caused to be stored on users' devices—and to be transmitted to Third Parties—was not authorized by Plaintiffs and Class members, and, in fact, those Website users specifically chose to decline or reject cookies, including personalized advertising, analytics, and social media cookies, as well as all those cookies associated with the sale or sharing of users' personal information.

174. Plaintiffs and the Class members had an objectively reasonable expectation of privacy surrounding their Private Communications on the Website based on Defendant's promise that users could opt out of, decline, or otherwise reject the sale of their personal information, and all third-party cookies involved with that sale, including at least all personalized advertising, analytics, and social media cookies, by adjusting the toggle switch to do so, as well as state criminal and civil laws designed to protect individual privacy.

175. Defendant's intentional intrusion into Plaintiffs' and other users' Private Communications would be highly offensive to a reasonable person given that Defendant represented that Website users could adjust the "Do not sell my personal information" toggle switch, thereby opting out of, declining, or rejecting such cookies, including at least all personalized advertising, analytics, and social media cookies, when, in fact, Defendant caused such third-party cookies to be stored on consumers' devices and browsers, and to be transmitted to third parties, even when consumers declined or rejected all such cookies. Indeed, Plaintiffs and Class members reasonably expected, based on Defendant's false representations, that when they declined or rejected cookies and tracking technologies, including at least all those personalized advertising, analytics, and social media cookies associated with the sale of users' personal information, Defendant would not cause such third-party cookies to be stored on their devices or permit the Third Parties to obtain their Private Communications on the Website, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is

located in California.

176. Defendant's conduct was intentional and intruded on Plaintiffs' and users' Private Communications on the Website.

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

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

179. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' declination or rejection of the Website's use of cookies that sell or share their personal information. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

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

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

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

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

182. Defendant is a "person" within the meaning of California Penal Code § 631.

183. The Third Parties' cookies—as well as the software code of the Third Parties responsible for placing the cookies and transmitting data from user devices to the Third Parties—

constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA (and, even if they do not, Defendant's deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of "any other manner").

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

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

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

187. At all relevant times, by their cookies and corresponding software code, the Third Parties, willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiffs and Class members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

188. The Private Communications of Plaintiffs and Class members, on the one hand, and Defendant, on the other, that the Third Parties automatically intercepted directly

communicates the Website user's affirmative decisions, actions, choices, preferences, and activities, which constitute the "contents" of electronic communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—including whether a user is located in California.

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

190. Plaintiffs and Class members did not provide their prior consent to the Third Parties' intentional access, interception, reading, learning, recording, collection, and usage of Plaintiffs' and Class members' electronic communications. Nor did Plaintiffs and Class members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties' conduct. On the contrary, Plaintiffs and Class members expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic communications by choosing to decline or reject all such cookies by adjusting the "Do not sell my personal information" toggle switch in the popup cookie consent banner.

191. The wiretapping of Plaintiffs and Class members occurred in California, where Plaintiffs and Class members accessed the Website and where the Third Parties—as caused by Defendant—routed Plaintiffs' and Class members' electronic communications to Third Parties' servers. Among other things, the cookies, as well as the software code responsible for placing the cookies and transmitting them and other Private Communications to the Third Parties, resided on Plaintiffs' California-located device. In particular, the user's California-based device, after downloading the software code from the Third Parties' servers, (i) stored the code onto the user's disk; (ii) converted the code into machine-executable format; and (iii) executed the code, causing the transmission of data (including cookie data) to and from the Third Parties.

192. Plaintiffs and Class members have suffered loss by reason of these violations,

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

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

194. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein including, but not limited to, permitting third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Plaintiffs, Class members, and the general public continue to be at risk because Plaintiffs, Class members, and the general public frequently use the internet to search for information and content related to personal health and wellness. Plaintiffs, Class members, and the general public continue to desire to use the internet for that purpose. Plaintiffs, Class members, and the general public have no practical way to know if their request to decline or reject the sale of their personal data, including at least all third-party analytics and advertising cookies and tracking technologies, will be honored and/or whether Defendant will permit third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant and will continue to do so unless and until enjoined.

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)

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

196. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to 638, includes the following statement of purpose:

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

197. California Penal Code Section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

198. A "pen register" is a "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).

199. The Third Parties' cookies and the corresponding software code installed by Defendant on its Website are each "pen registers" because they are "device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information"—including, the IP address and user-agent information—from the electronic communications transmitted by Plaintiff's and the Class's computers or devices. Cal. Penal Code § 638.50(b).

200. At all relevant times, Defendant caused pen registers (e.g., the Third Party software code and cookies) to be placed on Plaintiffs' and Class members' browsers and devices. This software code established and maintained network connections between the users' devices and the Third Parties, and also caused cookies, user data and metadata, and addressing and networking information (including, without limitation, IP addresses, port numbers, protocol-level metadata, HTTP request header metadata, and user-agent information), to be transmitted to the Third Parties.

201. Some of the information collected by the Third Parties' cookies and the corresponding software, including IP addresses and user-agent information, does not constitute the content of Plaintiff's and the Class members' electronic communications with the Website).

202. Plaintiffs and Class members did not provide their prior consent to Defendant's use of third-party cookies and the corresponding software. On the contrary, Plaintiffs and the

Class members informed Defendant that they did not consent to the Website's use of third-party cookies by adjusting the "Do not sell my personal information" toggle switch in the popup cookie consent banner.

203. Defendant did not obtain a court order to install or use the third-party cookies and corresponding software to track and collect Plaintiffs' and Class member's IP addresses and user-agent information.

204. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered losses and were damaged in an amount to be determined at trial.

205. Pursuant to Penal Code § 637.2(a)(1), Plaintiffs and Class members are also entitled to statutory damages of $5,000 for each of Defendant's violations of § 638.51(a).

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

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

207. Defendant fraudulently and deceptively informed Plaintiffs and Class members that they could opt out of, decline, or otherwise reject the sale or sharing of their personal information, and all cookies involved with that sale or sharing, including at least all personalized advertising, analytics, and social media cookies, by adjusting the toggle switch to do so in the popup cookie consent banner.

208. However, despite Defendant's representations otherwise, Defendant caused third-party cookies and software code to be stored on consumers' devices, and to be transmitted to the Third Parties alongside Private Communications, even after users adjusted the "Do not sell my personal information" toggle switch in the popup cookie consent banner. These cookies and corresponding software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' Private Communications, even when consumers had previously chosen to opt out of, decline, or reject all such cookies.

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

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

effectuated those choices.

211. Defendant and/or its agents configured and managed which technologies loaded and transmitted data before and after a user disabled third party cookies, including through consent management settings and/or platforms, tag-management rules, and related implementation choices under Defendant's control. On information and belief, Defendant operated, controlled, configured, approved, or maintained settings that permitted the Third Parties' tracking technologies to continue collecting users' Private Communications even after users adjusted the "Do not sell my personal information" toggle switch in the popup cookie consent banner and opt out of the collection, use, sale, and/or sharing of their Private Communications.

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

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

personalization, attribution, and/or website performance purposes.

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

215. On information and belief, Defendant either knew its representations regarding users' ability to adjust the "Do not sell my personal information" toggle switch in the popup cookie consent banner and opt out of data sharing were false, lacked any reasonable basis for believing those representations were, or made those representations carelessly and recklessly despite information available to Defendant demonstrating that users' data continued to be collected and transmitted to the Third Parties after users attempted to opt out

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

217. Plaintiffs and Class members relied to their detriment on Defendant's misrepresentations and fraudulent omissions.

218. Plaintiffs and Class members have suffered an injury-in-fact, including the loss of money and/or property, as a result of Defendant's unfair, deceptive, and/or unlawful practices, including the unauthorized interception of their Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, which have value as demonstrated by the

use and sale of consumers' browsing activity, as alleged above. Plaintiffs and Class members have also suffered harm in the form of diminution of the value of their private and personally identifiable information and communications.

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

220. Defendant's representation that consumers could decline or reject all cookies and tracking technologies associated with the selling or sharing of users' personal information (including all personalized advertising, analytics, and social media cookies) if they adjusted the "Do not sell my personal information" toggle switch in the popup cookie consent banner was untrue. Again, had Plaintiffs and Class members known these facts, they would not have used the Website. Moreover, Plaintiffs and Class members reviewed the popup cookie consent banner prior to their interactions with the Website. Had Defendant disclosed that it caused third-party cookies to be stored on Website visitors' devices that are related to personalized advertising, analytics, and social media, and/or share information with or sell user personal data to third parties, even after they choose to opt out of such sales, and all third-party cookies, Plaintiffs and Class members would have noticed it and would not have interacted with the Website.

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

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

223. As a direct and proximate result of Defendant's misrepresentations and/or omissions, Plaintiffs and Class members have suffered damages, as alleged above, and are

entitled to just compensation, including monetary damages.

224. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' declination or rejection of the Website's use of all cookies associated with the sale or sharing of their personal information. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Sixth Cause of Action: Unjust Enrichment

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

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

227. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could opt out of, decline, or reject the sale of their personal information, including all third-party personalized advertising, analytics, and social media cookies, and by permitting the Third Parties to store and transmit cookies on Plaintiffs' and Class members' devices and browsers, which permitted the Third Parties to track and collect users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even after Class members declined or rejected such cookies.

228. Plaintiffs and Class members' Private Communications, including their personal data, have conferred an economic benefit on Defendant.

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

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

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

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

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

234. Plaintiffs plead this claim separately, as well as in the alternative, to their other claims, as without such claims Plaintiffs would have no adequate legal remedy.

PRAYER FOR RELIEF

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

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

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

C. An award of punitive damages;

D. An award of nominal damages;

E. An order for full restitution;

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

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

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

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

Dated: June 5, 2026

GUTRIDE SAFIER LLP

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

Attorneys for Plaintiffs