

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 Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

STACY PENNING, an individual, on behalf of
himself, the general public, and those similarly
situated,

Plaintiff,

v.

NVIDIA CORPORATION,

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

1

2

3 INTRODUCTION 4

4 THE PARTIES..... 6

5 JURISDICTION AND VENUE 6

6 SUBSTANTIVE ALLEGATIONS 6

7

8 A. Defendant Programmed the Website to Include Third-Party Resources that Utilize Cookie Trackers..... 6

9

10 B. Defendant Falsely Informed Users That They Could Decline the Website’s Use of “All” Cookies. 12

11 C. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant’s Website. 22

12 1. Facebook Cookies..... 22

13 2. Google Cookies..... 27

14 3. TikTok Cookies 34

15 4. Adobe Cookies..... 40

16 5. LiveRamp Cookies..... 45

17 6. Taboola Cookies 47

18 7. Salesforce Cookies..... 49

19 8. Additional Third Party Cookies 50

20 D. The Private Communications Collected are Valuable. 58

21

22 PLAINTIFF’S EXPERIENCES 59

23

24 CLASS ALLEGATIONS 63

25

26 CAUSES OF ACTION..... 65

27

28 First Cause of Action: Invasion of Privacy..... 65

Second Cause of Action: Intrusion Upon Seclusion..... 68

Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631) 70

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)..... 75

Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation..... 76

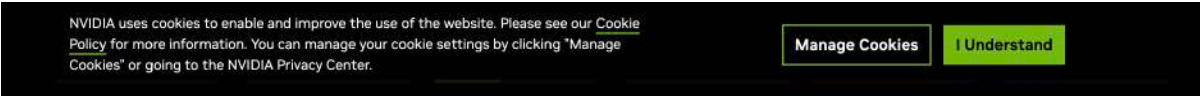
1 Sixth Cause of Action: Unjust Enrichment..... 79

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1
2 Plaintiff Stacy Penning (“Plaintiff”) brings this action on behalf of himself, the general
3 public, and all others similarly situated against NVIDIA Corporation (“Defendant” or
4 “NVIDIA”). Plaintiff’s allegations against Defendant are based upon information, belief and
5 upon investigation of Plaintiff’s counsel, except for allegations specifically pertaining to
6 Plaintiff, which are based upon Plaintiff’s personal knowledge.

7 INTRODUCTION

8 1. This Class Action Complaint concerns an egregious privacy violation and total
9 breach of consumer trust in violation of California law. When consumers visit Defendant’s
10 ecommerce website (www.nvidia.com, the “Website”), Defendant displays to them a popup
11 cookie consent banner. Defendant’s cookie banner discloses that the Website uses cookies but
12 expressly gives users the option to control how they are tracked and how their personal data is
13 used. Defendant assures visitors that they can choose to “Manage Cookies” as shown in the
14 following screenshot:

15  NVIDIA uses cookies to enable and improve the use of the website. Please see our [Cookie Policy](#) for more information. You can manage your cookie settings by clicking “Manage Cookies” or going to the NVIDIA Privacy Center.

16 **Manage Cookies**

I Understand

17 2. Like most internet websites, Defendant designed the Website to include
18 resources and programming scripts from third parties that cause those parties to place cookies
19 and other similar tracking technologies on visitors’ browsers and devices and/or transmit
20 cookies along with user data. However, unlike other websites, Defendant’s Website offers
21 consumers a choice to browse without being tracked, followed, and targeted by third party data
22 brokers and advertisers. But, Defendant’s promises are outright lies, designed to lull users into
23 a false sense of security. Even after users elect to “Decline All” cookies in the Cookie Settings
24 window, Defendant surreptitiously causes several third parties—including Meta Platforms, Inc.
25 (formerly Facebook), Google LLC (DoubleClick), ByteDance Ltd. (TikTok), Adobe, Inc.
26 (omtrcd.net), LiveRamp Holdings, Inc. (rlcdn.com), Taboola.com, Ltd., Salesforce, Inc.
27 (Evergage), PubMatic, Inc., Microsoft Corp. (AppNexus), LinkedIn Corporation (a subsidiary
28 of Microsoft Corp.), X Corp. (Twitter), Dun & Bradstreet Holdings, Inc. (Eyeota), Yahoo, Inc.,

1 NextRoll, Inc. (Adroll.com), Magnite, Inc. (Rubicon Project), Index Exchange, Inc. (Casale
2 Media), Bidswitch, Inc., TripleLift, Inc. (3lift.com), Teads Holding Co. (Outbrain)
3 (outbrain.com), and OpenX Technologies, Inc. (the “Third Parties”) —to place and/or transmit
4 cookies that track users’ website browsing activities and eavesdrop on users’ private
5 communications on the Website.

6 3. Contrary to their express declination of cookies and tracking technologies on the
7 Website, Defendant nonetheless caused cookies, including the Third Parties’ cookies, to be
8 sent to Plaintiff and other visitors’ browsers, stored on their devices, and transmitted to the
9 Third Parties along with user data. These third-party cookies permitted the Third Parties to
10 track and collect data in real time regarding Website visitors’ behaviors and communications,
11 including their browsing history, visit history, website interactions, user input data,
12 demographic information, interests and preferences, shopping behaviors, device information,
13 referring URLs, session information, user identifiers, and/or geolocation data—including
14 whether a user is located in California.

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

21 5. This type of tracking and data sharing is exactly what the Website visitors who
22 clicked or selected the “Decline All” button and/or by toggled off “Performance Cookies” and
23 “Advertising Cookies” in the Website’s Cookie Settings window sought to avoid. Defendant
24 falsely told Website users that it respected their privacy and that they could avoid tracking and
25 data sharing when they browsed the Website. Despite receiving notice of consumers’ express
26 declination of consent, Defendant defied it and violated state statutes and tort duties owed to
27 Plaintiff and those similarly situated Website users.

1 **THE PARTIES**

2 6. Plaintiff Stacy Penning is, and was at all relevant times, an individual and
3 resident of El Cerrito, California. Plaintiff intends to remain in California and makes his
4 permanent home there.

5 7. Defendant NVIDIA Corporation is a Delaware corporation with its headquarters
6 and principal place of business in Santa Clara, California.

7 **JURISDICTION AND VENUE**

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

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

17 10. Further, the Private Communications and data which Defendant causes to be
18 transmitted to Third Parties are routed through servers located in California.

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

22 12. Plaintiff accordingly alleges that jurisdiction and venue are proper in this Court.

23 **SUBSTANTIVE ALLEGATIONS**

24 **A. Defendant Programmed the Website to Include Third-Party Resources that**
25 **Utilize Cookie Trackers.**

26 13. Every website, including the Website, is hosted by a server that sends and
27 receives communications in the form of HTTP requests, such as “GET” or “POST” requests, to
28 and from Internet users’ browsers. For example, when a user clicks on a hyperlink on the

1 Website, the user's browser sends a "GET" request to the Website's server. The GET request
2 tells the Website server what information is being requested (e.g., the URL of the webpage
3 being requested) and instructs the Website's server to send the information back to the user
4 (e.g., the content of the webpage being requested). When the Website server receives an HTTP
5 request, it processes that request and sends back an HTTP response. The HTTP request
6 includes the client's IP address so that the Website server to knows where to send the HTTP
7 response.

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

14 15. As a result, Defendant knew that the devices used by Plaintiff and Class
15 members to access the Website were located in California.

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

23 17. The Website causes users' devices to store and/or transmit both first-party and
24 third-party tracking cookies. Cookies are small text files sent by a website server to a user's
25 web browser and stored locally on the user's device. As described below, cookies generally
26 contain a unique identifier which enables the website to recognize and differentiate individual
27 users. Cookie files are sent back to the website server along with HTTP requests, enabling the
28

1 website to identify the device making the requests, and to record a session showing how the
2 user interacts with the website.

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

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

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

- 20 • **Browsing History:** Information about the webpages a Website user visits,
21 including the URLs, titles, and keywords associated with the webpages viewed,
22 time spent on each page, and navigation patterns;
- 23 • **Visit History:** Information about the frequency and total number of visits to the
24 Website;
- 25 • **Website Interactions:** Data on which links, buttons, or ads on the Website that
26 a user clicks;

- 1 • **User Input Data:** The information the user entered into the Website’s form
2 fields, including search queries, the user’s name, age, gender, email address,
3 location, and/or payment information;
- 4 • **Demographic Information:** Inferences about age, gender, and location based
5 on browsing habits and interactions with Website content;
- 6 • **Interests and Preferences:** Insights into user interests based on the types of
7 Website content viewed, products searched for, or topics engaged with;
- 8 • **Shopping Behavior:** Information about the Website products viewed or added
9 to shopping carts;
- 10 • **Device Information:** Details about the Website user’s device, such as the type
11 of device (mobile, tablet, desktop), operating system, and browser type;
- 12 • **Referring URL:** Information about the website that referred the user to the
13 Website;
- 14 • **Session Information:** Details about the user’s current Website browsing
15 session, including the exact date and time of the user’s session, the session
16 duration and actions taken on the Website during that session;
- 17 • **User Identifiers:** A unique ID that is used to recognize and track a specific
18 Website user across different websites over time; and/or
- 19 • **Geolocation Data:** General location information based on the Website user’s IP
20 address or GPS data, if accessible, including whether the user is located in
21 California.

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

24 21. Third-party cookies can be used for a variety of purposes, including
25 (i) analytics (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness
26 of marketing campaigns); (ii) personalization (e.g., remembering a user’s browsing history and
27 purchase preferences to enable product recommendations); (iii) advertising/targeting (e.g.,
28

1 delivering targeted advertisements based on the user’s consumer profile (i.e., an aggregated
2 profile of the user’s behavior, preferences, and demographics); and (iv) social media
3 integration (e.g., enabling sharing of users’ activities with social media platforms). Ultimately,
4 third-party cookies are utilized to boost website performance and revenue through the
5 collection, utilization, and dissemination of user data.

6 22. Defendant is a technology company best known for designing graphics
7 processing units (GPUs), which are widely used in gaming, professional visualization, data
8 centers, and artificial intelligence. In addition to hardware, NVIDIA develops software
9 platforms and systems for AI, machine learning, and accelerated computing. Defendant also
10 owns and operates the Website, which allows visitors to receive information about its hardware
11 and software products and purchase products. As they interact with the Website (e.g., by
12 entering data into forms, clicking on links, and making selections), Website users communicate
13 Private Communications to Defendant, including their browsing history, visit history, website
14 interactions, user input data, demographic information, interests and preferences, shopping
15 behaviors, device information, referring URLs, session information, user identifiers, and/or
16 geolocation data—including whether a user is located in California.

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

25 24. Defendant admitted that the Website allows third parties to collect user data
26 with cookies in its Privacy Policy as follows:
27
28

1 If you visit any of our NVIDIA websites, we or our third-party partners collect
2 information using cookies, web beacons, or log file information. Please see our Cookie
3 Policy for more details.¹

4 25. Further, Defendant explained the third-party cookies it used on the Website as
5 follows in its Cookie Policy:

6 A cookie is a small data file made up of letters and numbers which is placed by a
7 website on the device you use to access the Internet. Cookies serve different
8 purposes, and may be tied to personal information. At NVIDIA, we use cookies to
9 help deliver and improve our websites (such as NVIDIA.com, Geforce.com, and
10 Developer.nvidia.com) through information about website usage and settings, as
11 described below. How we use cookies is governed by this Cookie Policy and by
12 our Privacy Policy.²

13 26. Further, Defendant described the categories of cookies used on the Website as
14 follows in its Cookie Policy:

15 **Performance Cookies**

16 These cookies are used to better understand and optimize the web experience. These
17 cookies collect information such as pages visited or purchased made through our eStore.

18 **Advertising Cookies**

19 These cookies are used to personalize your web experience with relevant advertisements.
20 These cookies collect information such as pages visited or purchases made through our
21 eStore.

22 **Required Cookies**

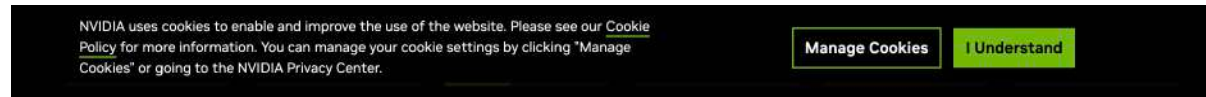
23 These cookies are required for the website to properly function on your device. These
24 cookies collect information such as location (for language settings), account
25 management, event registration, driver installs, or email preferences.

26 ¹ NVIDIA Privacy Policy (Effective date September 22, 2025) (available at
27 <https://www.nvidia.com/en-us/about-nvidia/privacy-policy>. Similar language has appeared in
28 prior versions of NVIDIA Privacy Policy.

² NVIDIA Website Cookie Policy (as it appeared on 7/4/2024) (available at
<https://www.nvidia.com/en-us/about-nvidia/cookie-policy/>) (the “Cookie Policy”). Defendant
has subsequently updated its Cookie Policy but, based on information and belief, this version
was in effect at the time of Plaintiff’s rejection of cookies on the Website.

1 **B. Defendant Falsely Informed Users That They Could Decline the Website’s**
2 **Use of “All” Cookies.**

3 27. When Plaintiff and other consumers in California visited the Website, the
4 Website immediately displayed to them a popup cookie consent banner. As shown in the
5 screenshot below, the cookie consent banner stated, “NVIDIA uses cookies to enable and
6 improve the use of the website...You can manage your cookie settings by clicking ‘Manage
7 Cookies’ or going to the NVIDIA Privacy Center.” Accordingly, the banner then purported to
8 provide users the opportunity to “Manage Cookies” by clicking the button as shown in the
9 following screenshot from the Website:



11 28. Plaintiff and other Website users who clicked or selected the “Manage Cookies”
12 button were then directed to Defendant’s “Cookie Settings” window. There, Defendant further
13 represented, “NVIDIA websites use cookies to deliver and improve the visitor experience.
14 Learn more about the cookies we use on our Cookie Policy page.” The “Cookie Settings”
15 window identified three categories of cookies in use on the Website, including “Performance
16 Cookies” and “Advertising Cookies,” each of which could be turned “off” by adjusting a
17 toggle or setting to do so. Defendant represented that “Required Cookies” are “required for the
18 site to function” and “cannot be turned off[.]” Besides the toggles or settings available to
19 decline specific categories of cookies, there was also a “Decline All” button that users could
20 click or select, as shown in the following screenshot:



25 29. Users who clicked or selected the “Decline All” button and/or toggled off
26 “Performance Cookies” and “Advertising Cookies,” thereby indicating their choice and/or
27 agreement to decline “All” cookies and tracking technologies in use on the Website, including
28 all Performance and Advertising cookies (other than those “Required Cookies” needed for the

1 Website to function), could then continue to browse the Website, as the popup cookie consent
2 banner and Cookie Settings window disappeared.

3 30. Defendant’s popup cookie consent banner and Cookie Settings window led
4 Plaintiff, and all those Website users similarly situated, to believe that they declined “All”
5 cookies and tracking technologies, especially those used to “understand where people most
6 engage with links” and “build a profile of [user] interests to show [users] relevant ads on other
7 sites.” The banner further reasonably led Plaintiff and those Website users similarly situated
8 to believe that Defendant would not allow third parties, through cookies, to access their
9 Private Communications with the Website, including their browsing history, visit history,
10 website interactions, user input data, demographic information, interests and preferences,
11 shopping behaviors, device information, referring URLs, session information, user identifiers,
12 and/or geolocation data, upon clicking or selecting the “Decline All” cookies button.

13 31. Defendant’s representations, however, were false. In truth, Defendant did not
14 abide by Plaintiff’s or other users’ wishes. When Plaintiff and other Website users clicked or
15 selected the “Decline All” cookies button and/or toggled off “Performance Cookies” and
16 “Advertising Cookies,” they provided notice to Defendant that they did not consent to the
17 placement or transmission of third-party cookies that would allow those parties to obtain their
18 Private Communications with the Website. Nevertheless, Defendant caused the Third Party
19 tracking cookies to be placed on Website users’ browsers and devices and/or transmitted to
20 the Third Parties along with user data.

21 32. In particular, when users clicked or selected the “Decline All” cookies button
22 and/or toggled off “Performance Cookies” and “Advertising Cookies, Defendant nonetheless
23 continued to cause the Third Parties’ cookies to be placed on users’ devices and/or transmitted
24 to the Third Parties along with user data, enabling them to collect user data in real time that
25 discloses Website visitors’ Private Communications, including browsing history, visit history,
26 website interactions, user input data, demographic information, interests and preferences,
27 shopping behaviors, device information, referring URLs, session information, user identifiers,
28

1 and/or geolocation data. In other words, even when consumers like Plaintiff tried to protect
2 their privacy by declining “All” cookies, Defendant failed to prevent cookies from being
3 transmitted to Third Parties, enabling them to track user behavior and communications.

4 33. Some aspects of the operations of the Third Party cookies on the Website can be
5 observed using specialized tools that log incoming and outgoing Website network
6 transmissions. The following screenshots, obtained using one such tool, show examples of the
7 Third Parties’ cookies being transmitted from a Website user’s device and browser to the Third
8 Parties even after the user clicked or selected the “Decline All” button on the Website’s Cookie
9 Settings window:

10
11
12
13
14
15
16
17
18
19 [REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.]
20
21
22
23
24
25
26
27
28

The screenshot shows the NVIDIA GeForce website on a desktop browser. The page features a dark theme with green accents. The main heading is "Graphics Cards" in white. Below it, there are two sections: "GeForce RTX 40 Series" and "GeForce RTX 30 Series", each with a "Learn More" button. The browser's network developer tool is open on the right side, displaying a list of network requests. The table below shows the details of these requests.

Name	Domain	Cookies
Pug?vcode=bz0yJnR5cGU9MSZjb2R...	image2.pubmatic.com	36
Pug?vcode=bz0yJnR5cGU9MSZjb2R...	image2.pubmatic.com	36
setuid?entity=172&code=NjM5MG...	ib.adnxs.com	7
setuid?entity=172&code=NjM5MG...	ib.adnxs.com	7
trigger/?id=161755414605325&ev=...	www.facebook.com	6
tr/?id=161755414605325&ev=Subsc...	www.facebook.com	6
wa/	px.ads.linkedin.com	6
trigger/?id=1928711947357163&ev=...	www.facebook.com	6
tr/?id=1928711947357163&ev=Pag...	www.facebook.com	6
trigger/?id=161755414605325&ev=...	www.facebook.com	6
tr/?id=161755414605325&ev=Page...	www.facebook.com	6
wa/	px.ads.linkedin.com	6
collect?v=2&fmt=js&pid=84497&ti...	px.ads.linkedin.com	6
trigger/?id=161755414605325&ev=...	www.facebook.com	6
tr/?id=161755414605325&ev=Subsc...	www.facebook.com	6
wa/	px.ads.linkedin.com	6
trigger/?id=161755414605325&ev=...	www.facebook.com	6
tr/?id=161755414605325&ev=Subsc...	www.facebook.com	6
wa/	px.ads.linkedin.com	6
trigger/?id=161755414605325&ev=...	www.facebook.com	6
tr/?id=161755414605325&ev=Subsc...	www.facebook.com	6
wa/	px.ads.linkedin.com	6
wa/	px.ads.linkedin.com	6
trigger/?id=1928711947357163&ev=...	www.facebook.com	6
tr/?id=1928711947357163&ev=Pag...	www.facebook.com	6
sync?nid=eyeota	sync.srv.stackadapt.com	6
trigger/?id=161755414605325&ev=...	www.facebook.com	6
tr/?id=161755414605325&ev=Page...	www.facebook.com	6
wa/	px.ads.linkedin.com	6
collect?v=2&fmt=js&pid=84497&ti...	px.ads.linkedin.com	6
collect?v=2&fmt=js&pid=84497&ti...	px4.ads.linkedin.com	5
collect?v=2&fmt=js&pid=84497&ti...	px4.ads.linkedin.com	5
RVXVWKJN7ZFAJEQ2WH4YF4?adrol...	ipv4.d.adroll.com	4
in?id=id%3A560-NBS-753%26token...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4

575 / 792 requests | 754 kB / 8.4 MB transferred | 19.9 MB / 38.4 MB resources

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

The screenshot displays the NVIDIA GeForce website at [nvidia.com/en-us/geforce/graphics-cards/](https://www.nvidia.com/en-us/geforce/graphics-cards/). The page features a dark theme with green accents. The main heading is "Graphics Cards". Below this, there are two primary sections: "GeForce RTX 40 Series" and "GeForce RTX 30 Series", each with a "Learn More" button. A "Feedback" button is visible on the right side of the page.

The browser's network developer tool is open, showing a list of network requests. The table below represents the data from the network tool:

Name	Domain	Cookies
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
RVXVVKJN7ZFAJEQ2WH4YF4?adrol...	d.adroll.com	4
JUWZDLBKWFDCNT75AR2KST?adrol...	d.adroll.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=173d...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=4ee2f...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=3b24...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=8817...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=8ae7...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=0d89...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=3dac...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=e93c...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=8e37...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=238c...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
imsync.ashx?pi=3644040318609260...	ml314.com	4
RVXVVKJN7ZFAJEQ2WH4YF4?adrol...	ipv4.d.adroll.com	4
in?id=id%3A560-NBS-753%26token...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4

575 / 792 requests | 754 kB / 8.4 MB transferred | 19.9 MB / 38.4 MB resources

The screenshot shows the NVIDIA GeForce website with a browser developer tools network tab open. The network tab displays a list of requests, including several to adroll.com and analytics.twitter.com. The requests are filtered by domain and show various tracking parameters.

Name	Domain	Cookies
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
out?adroll_fpc=07bc1c68bc659c317...	d.adroll.com	4
RVXVWKJNZFAJEQ2WH4YF4?adrol...	d.adroll.com	4
JUWZDLBKWFDCTN75AR2KST?adrol...	d.adroll.com	4
adsct?bci=5&eci=2&event_id=dab1...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=c1cec...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=9dfe...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=6a27...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=3852...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=d45f...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=aad5...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=e64f...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=cba9...	analytics.twitter.com	4
adsct?bci=5&eci=2&event_id=c397...	analytics.twitter.com	4
adsct?bci=5&eci=3&event=%7B%7...	analytics.twitter.com	4
iframe_content.html?adroll_fpc=07b...	x.adroll.com	3
1041695361?random=17196038031...	td.doubleclick.net	3
igs?advertisable=JUWZDLBKWFDCT...	x.adroll.com	3
igs?advertisable=JUWZDLBKWFDCT...	x.adroll.com	3
js_tracking?url=https%3A%2F%2Fw...	tags.srv.stackadapt.com	3
trigger?fpc=07bc1c68bc659c31739e...	x.adroll.com	3
tap.php?v=194538&nid=3644&put...	pixel.rubiconproject.com	3
rum?cm_dsp_id=105&external_user...	dsum-sec.casalemedia.c...	3
sync?dsp_id=44&user_id=NjM5MG...	x.bidswitch.net	3
saq_pxl?uid=8KPnb9mQLcH0mq2p...	tags.srv.stackadapt.com	3
1041695361/?random=1719603823...	googleads.g.doubleclick...	3
1041695361/?random=1719603823...	googleads.g.doubleclick...	3
62d5c127677d11008e98da2b	ws.zoominfo.com	3
events.js	tags.srv.stackadapt.com	3

577 / 794 requests | 755 kB / 8.4 MB transferred | 19.9 MB / 38.4 MB resources

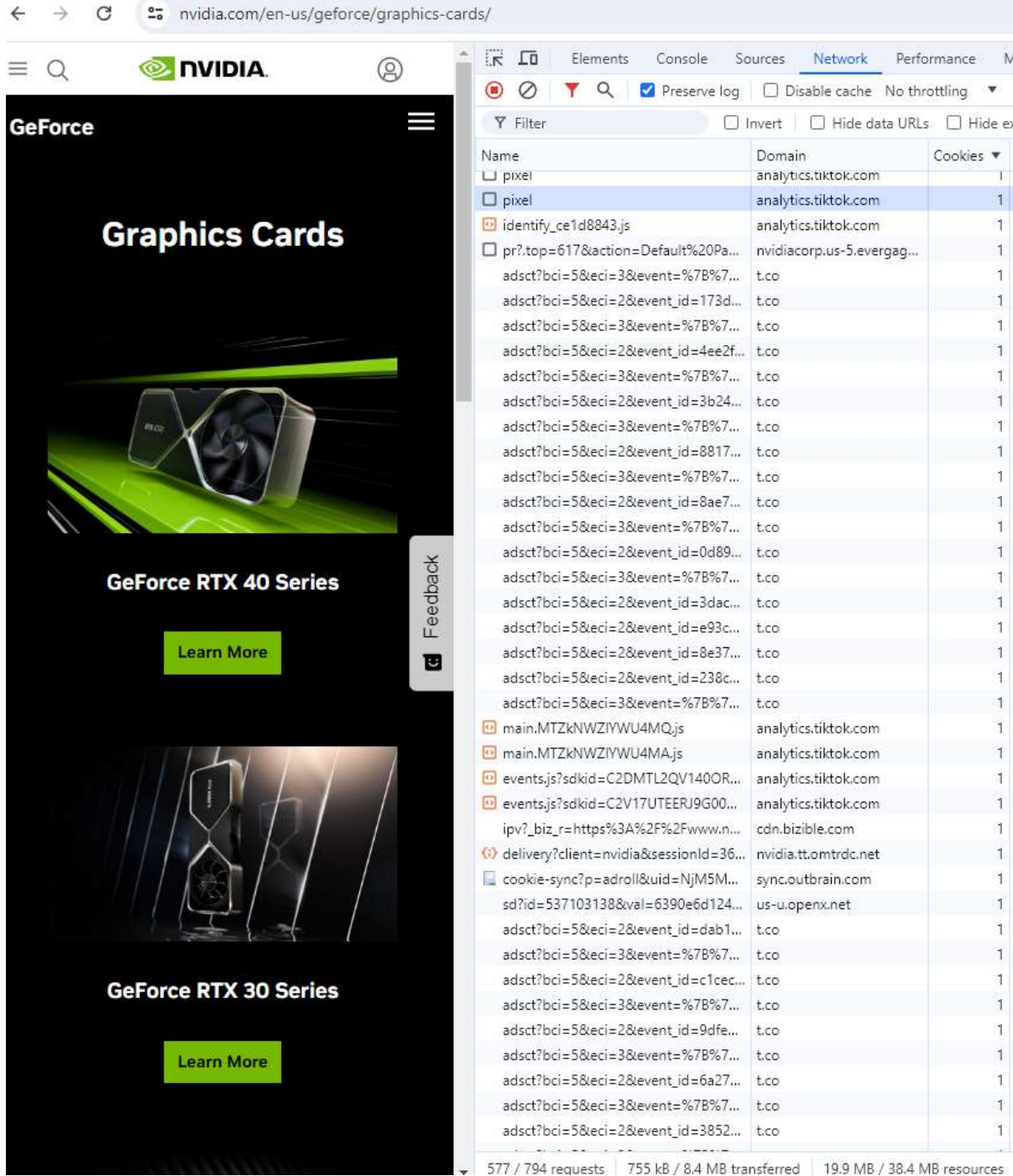
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

The screenshot displays the NVIDIA GeForce website interface. The main heading is 'Graphics Cards'. Below it, there are two featured sections: 'GeForce RTX 40 Series' and 'GeForce RTX 30 Series', each with a 'Learn More' button. A 'Feedback' button is visible on the right side of the page.

The network developer tool is open, showing a list of requests. The table below represents the data from the network tool:

Name	Domain	Cookies
pixel.gif?cs=22:1,20:1&fp=0771e169...	aorta.clickagy.com	2
pixel.gif?cs=33:-1,37:1,48:-1,52:1,38:...	aorta.clickagy.com	2
pixel?pid=r8hrb20&t=gif	ps.eyeota.net	2
match?bid=tpm4omv&uid=nPqDLn...	ps.eyeota.net	2
pixel.gif?clkgypv=jstag&wvs=1	aorta.clickagy.com	2
data	aorta.clickagy.com	2
xuid?mid=4714&xuid=NjM5MGU2Z...	eb2.3lift.com	2
rtb-h?taboola_hm=NjM5MGU2ZDEy...	sync.taboola.com	2
sync?_origin=1&uid=NjM5MGU2ZD...	ups.analytics.yahoo.com	2
377928.gif?partner_uid=6390e6d124...	idsync.rldcn.com	2
delivery?client=nvidia&sessionId=36...	nvidia.tt.omtrdc.net	1
etail	api.nvidia.partners	1
ipv?_biz_r=https%3A%2F%2Fwww.n...	cdn.bizible.com	1
retailer-newegg-ca.png	assets.nvidia.partners	1
retailer-newegg.png	assets.nvidia.partners	1
Micro-Center.png	assets.nvidia.partners	1
memory-express-retailer-logo.png	assets.nvidia.partners	1
retailer-canada-computers.png	assets.nvidia.partners	1
retailer-costco.png	assets.nvidia.partners	1
retailers_bestbuy_new.png	assets.nvidia.partners	1
retailer-best-buy-ca.png	assets.nvidia.partners	1
retailer-b-and-h.png	assets.nvidia.partners	1
retailer-antonline-white.png	assets.nvidia.partners	1
Amazon.png	assets.nvidia.partners	1
loading16.gif	www.nvidia.partners	1
nvidia-brand.css	www.nvidia.partners	1
l0g045d8ns2k	www.nvidia.partners	1
delivery?client=nvidia&sessionId=36...	nvidia.tt.omtrdc.net	1
ipv?_biz_r=https%3A%2F%2Fwww.n...	cdn.bizible.com	1
delivery?client=nvidia&sessionId=36...	nvidia.tt.omtrdc.net	1
pr?.top=29134&action=Default%20...	nvidiacorp.us-5.evergag...	1
act	analytics.tiktok.com	1
act	analytics.tiktok.com	1
act	analytics.tiktok.com	1
cookie-sync?p=adroll&uid=NjM5M...	sync.outbrain.com	1
sd?id=537103138&val=6390e6d124...	us-u.openx.net	1
pixel	analytics.tiktok.com	1
pixel	analytics.tiktok.com	1
pixel	analytics.tiktok.com	1

577 / 794 requests | 755 kB / 8.4 MB transferred | 19.9 MB / 38.4 MB resources



34. The screenshots above show the “Network” tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user’s browser and various third party websites while the user visited and interacted with Defendant’s Website at https://www.nvidia.com. The screenshots depict only network traffic occurring *after* the user declined “All” cookies using the Cookie Settings window. As shown above, despite the user’s declination of “All” cookies, the user’s interactions with the Website resulted in the user’s

1 browser making a large number of GET and POST HTTP requests to third party web domains
2 such as www.facebook.com, td.doubleclick.net, analytics.tiktok.com, omtred.net, and many
3 others. As further shown in the right-hand column of the screenshots, the user's browser sent
4 cookies along with those HTTP requests to the third parties. These screenshots demonstrate
5 that the Website caused third-party cookie data and users' Private Communications to be
6 transmitted to Third Parties, even after consumers declined all cookies and tracking
7 technologies by clicking or selecting the "Decline All" cookies button. All of these network
8 calls are made to the Third Parties without the user's knowledge, and despite the user's
9 declination of "All" cookies.

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

15 36. As users interact with the Website, even after clicking or selecting the "Decline
16 All" cookies button, thereby declining the use of cookies and similar technologies for
17 performance analysis and advertising, as well as the sale or sharing of the user's personal
18 information with third parties for such functions, or other purposes, more data regarding users'
19 behavior and communications are sent to third parties, alongside the cookie data. The third-
20 party cookies that Defendant wrongfully allows to be stored on users' devices and browsers,
21 and to be transmitted to the Third Parties, cause the Third Parties to track and collect data on
22 users' behaviors and communications, including Private Communications, on the Website.
23 Because third-party cookies cause Third Parties to track users' behavior across the Internet and
24 across time, user data can be correlated and combined with other data sets to compile
25 comprehensive user profiles that reflect consumers' behavior, preferences, and demographics
26 (including psychological trends, predispositions, attitudes, intelligence, abilities, and
27 aptitudes). These Third Parties monetize user profiles for advertising, sales, and marketing
28

1 purposes to generate revenue and target advertising to Internet users. Advertisers can gain deep
2 understanding of users’ behavioral traits and characteristics and target those users with
3 advertisements tailored to their consumer profiles and audience segments.

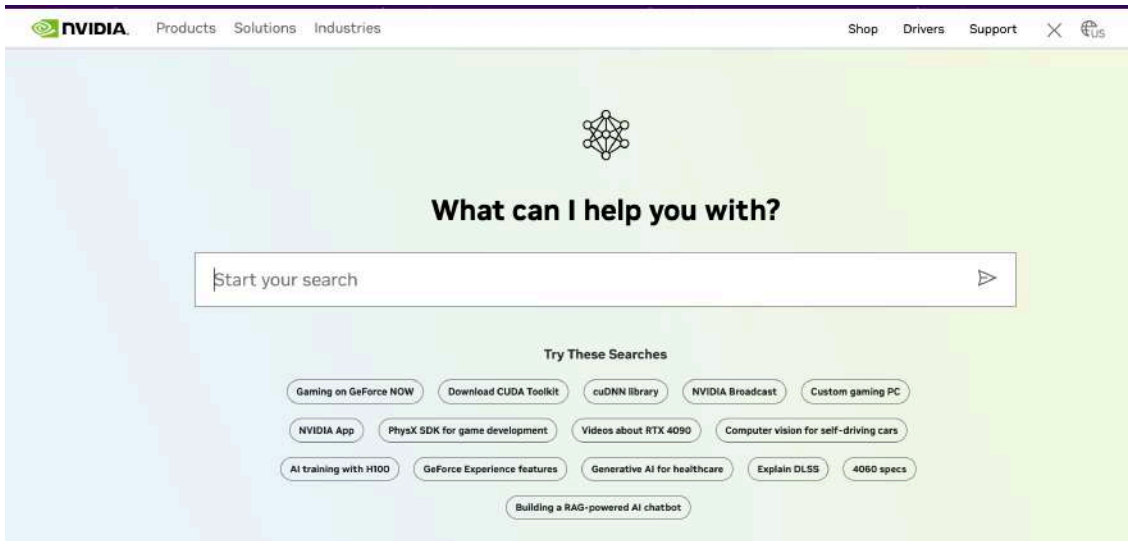
4 37. The Third Party code that the Website causes to be loaded and executed by the
5 user’s browser becomes a wiretap when it is executed because it causes the Third Parties—
6 separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop
7 upon, record, extract data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

12 **C. The Private Communications Collected As a Result of Third Party Cookies**
13 **Transmitted When Visiting Defendant’s Website.**

14 **1. The Website Causes the Interception of the Contents of**
15 **Communications**

16 38. The Website includes search bars and forms where users input information. For
17 example, below are screenshots of the search bar on the Website where users can type into the
18 search bar to cause the Website to search its contents.

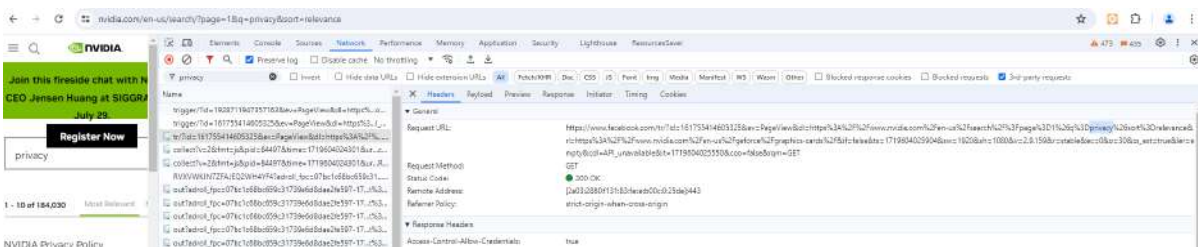




39. When Plaintiff and other Website users input the information into the search bar, they are intending to communicate with the Website the contents of the search to receive the information they are interested in.

40. Instead, the software on the Website causes the contents of the communication to be intercepted while in transit.

41. For example, the Website sends users' search strings to Facebook—even after consumers have declined all cookies. In the example below, the test string “privacy” was sent to Facebook along with cookie data:

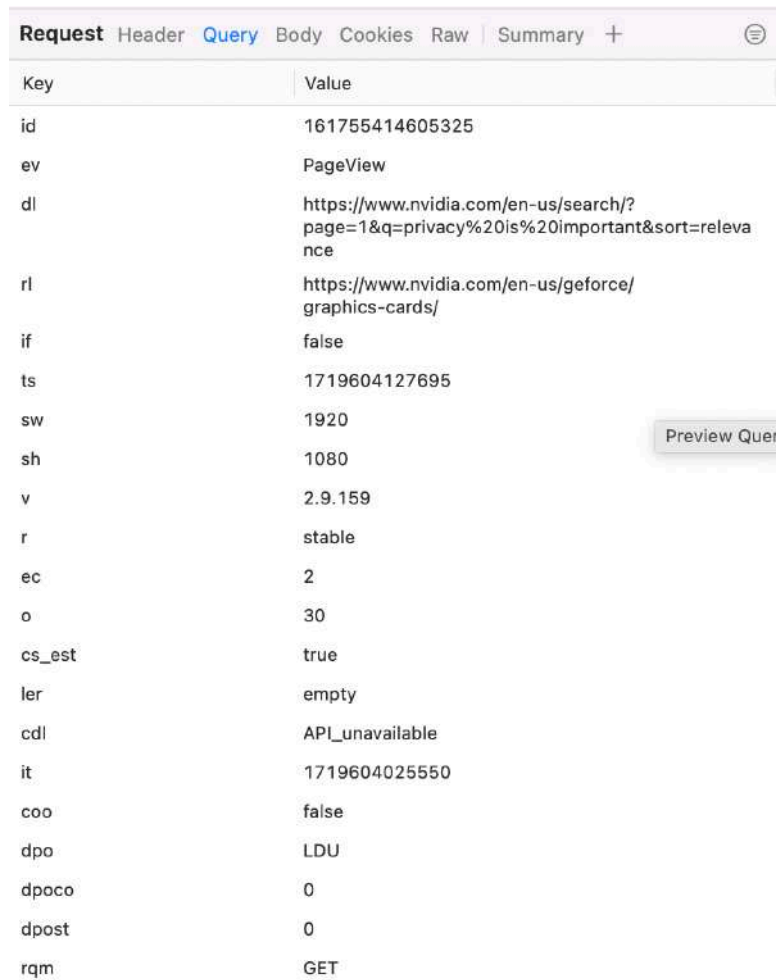


2. Facebook Cookies

42. Defendant causes third-party cookies to be transmitted to and from Website users' browsers and devices to and from the facebook.com domain, even after users elect to

1 “Decline All” cookies (including all Performance and Advertising cookies) and/or to toggle off
 2 “Performance Cookies” and “Advertising Cookies”. This domain is associated with Meta’s
 3 digital advertising and analytics platform that collects user information via cookies to assist
 4 Meta in performing data collection, behavioral analysis, user retargeting, and analytics.³ Meta
 5 serves targeted ads to web users across Meta’s ad network, which spans millions of websites
 6 and apps.

7 43. Cookies help Meta track whether users complete specific actions after
 8 interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics
 9 that advertisers use to measure ad campaign performance. For example, the Website causes the
 10 following data to be sent to Meta when the user enters a search term into the Nvidia Website:



Request	Header	Query	Body	Cookies	Raw	Summary	+	⊖
Key	Value							
id	161755414605325							
ev	PageView							
dl	https://www.nvidia.com/en-us/search/?page=1&q=privacy%20is%20important&sort=relevance							
rl	https://www.nvidia.com/en-us/geforce/graphics-cards/							
if	false							
ts	1719604127695							
sw	1920							
sh	1080							
v	2.9.159							
r	stable							
ec	2							
o	30							
cs_est	true							
ler	empty							
cdl	API_unavailable							
it	1719604025550							
coo	false							
dpo	LDU							
dpoco	0							
dpost	0							
rqm	GET							

28 ³ <https://www.facebook.com/privacy/policies/cookies/>.

1 44. The “ev” parameter is short for “event.” In this instance, the event is a
 2 “PageView.”

3 45. The “dl” parameter is the “Document Location.” It tells Facebook the specific
 4 webpage on which the Event occurred – in this case, [https://www.nvidia.com/en-
 5 us/search/?page=1&q=privacy%20is%20important&sort=relevance](https://www.nvidia.com/en-us/search/?page=1&q=privacy%20is%20important&sort=relevance). This also discloses to
 6 Facebook the user’s search query: “privacy is important.”

7 46. The “ts” parameter corresponds to a “Timestamp,” and tells Facebook the exact
 8 time—down to the millisecond—at which the user viewed the page.

9 47. The “sw” and “sh” parameters stand for “screen width” and “screen height,”
 10 and correspond to the display the user was viewing when the event was recorded.

11 48. Cookies are sent along with all data transmissions to Meta. For instance, the
 12 following cookies were sent along with the AddToCart event:

Key	Value
sb	pQI9ZkmdCAXYrQSQXngSSMep
datr	pQI9Zu6rOGZxJLTz7YrqaTVV
c_user	100076133960803
ps_n	1
xs	11%3Adi1FNrtx5ix0HA%3A2%3A1715274410%3A-1%3A-1%3A%3AAcVh1547GCKJnGyv jMaUEMTJP0UrmrTFxLBSDo-pqw
fr	1jvLdroEbgYmCRu9g.AWV2lzhppEBpcTVNrh DCqIaQVU.Bmfvv1..AAA.0.0.BmfwGM.AWXx M7L0HEQ

13
 14
 15
 16
 17
 18
 19
 20
 21
 22 49. Defendant identified the fr cookie shown above as an “Advertising Cookie”
 23 used on the Website in the Cookie Policy and described its purpose as follows:
 24

fr	Persistent cookie (expires after 1 month)	Third party (Facebook)	Used by Facebook to enable ad delivery or retargeting.
----	---	------------------------	--

25
 26 50. The c_user cookie shown above enables Facebook to identify a specific user
 27 when they are logged in to their account. The c_user cookie stores a user’s unique ID, which is
 28

1 associated with their Facebook profile. This ID enables Facebook to track user interactions on
2 its platform and across sites that use Facebook plugins, such as adding items to a cart, clicking
3 “Like” buttons, or engaging with comment sections. When combined with other data sent to
4 the Facebook domain, this cookie allows Meta to track users’ browsing activities. Facebook
5 uses this data for various purposes, such as personalizing content, enhancing ad targeting
6 accuracy, and refining its user experience.

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

12 52. The facebook.com cookies allow Meta to obtain and store at least the following
13 user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data,
14 (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii)
15 device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii)
16 geolocation data (including IP addresses).⁶

17 53. Meta utilizes the data collected through the facebook.com cookies for its own
18 purposes, including by using the data to tailor content and target advertisements to users. This
19 includes practices such as (i) **Ad Targeting and Retargeting**, in which Meta uses the
20 facebook.com cookie to track users’ online behavior across different sites, building a profile
21 based on their browsing habits, purchases, and interactions. This profile enables Facebook to
22 deliver highly targeted ads within the Facebook ecosystem and on other sites that are part of
23 Facebook’s Audience Network; (ii) **Conversion Tracking**, in which Meta uses the
24 facebook.com cookie to enable business partners to track specific actions users take after
25 viewing or clicking on a Facebook ad, such as making a purchase or signing up for a

26 ⁴ *Id.*; <https://allaboutcookies.org/what-data-does-facebook-collect>

27 ⁵ <https://allaboutcookies.org/what-data-does-facebook-collect>.

28 ⁶ *Id.*

1 newsletter; (iii) **Audience Insights and Analytics**, in which Meta uses the facebook.com
2 cookie to provide data to businesses on user demographics, interests, and behaviors across their
3 sites and apps; and (iv) **Cross-Device and Cross-Platform Tracking**, in which Meta uses the
4 facebook.com cookie to support tracking users across devices and platforms, so that ads are
5 targeted consistently regardless of the device a user is on. This ensures that advertisers can
6 follow users across devices.

7 54. Further, along with all of this data, the Facebook software code that Defendant
8 causes to be stored on and executed by the user’s device causes the user’s “user-agent”
9 information to be sent to Facebook:

```
10 user-agent Mozilla/5.0 (Windows NT 10.0;  
11 Win64; x64) AppleWebKit/537.36  
12 (KHTML, like Gecko) Chrome/  
13 126.0.0.0 Safari/537.36
```

14 55. The “user-agent” corresponds to the device and browser that the user has used
15 to access the Website.

16 56. Finally, the data sent to Facebook contains the user’s IP address—which can be
17 used to determine a user’s geolocation, including whether they are located in California.

18 **3. Google Cookies**

19 57. Defendant also causes third party cookies to be transmitted to and from Website
20 users’ browsers and devices, even after users choose to “Decline All” cookies (including
21 Performance and Advertising cookies) and/or to toggle off “Performance Cookies” and
22 “Advertising Cookies,” to and from the doubleclick.net domain. This domain is associated
23 with Google LLC’s digital advertising and analytics platform that collects user information via
24 cookies to assist Google in performing data collection, behavioral analysis, user retargeting,
25 and analytics.⁷ Google serves targeted ads to web users across Google’s ad network, which
26

27 ⁷ See Our advertising and measurement cookies (available at
28 <https://business.safety.google/adscookies/>).

1 spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's
2 DoubleClick cookies.⁸ Google's cookies help it track whether users complete specific actions
3 after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic
4 metrics that advertisers use to measure ad campaign performance. Further, by identifying users
5 who have shown interest in certain products or content, Google's cookies cause its advertising
6 platform to enable advertisers to show relevant ads to those users when they visit other
7 websites within Google's ad network.⁹

8
9 58. Specifically, Google sends cookies when a web user visits a webpage that
10 shows Google Marketing Platform advertising products and/or Google Ad Manager ads.¹⁰
11 "Pages with Google Marketing Platform advertising products or Google Ad Manager ads
12 include ad tags that instruct browsers to request ad content from [Google's] servers. When the
13 server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google
14 Marketing Platform advertising products or Google Ad Manager ads for this to happen; it just
15 needs to include Google Marketing Platform advertising products or Google Ad Manager ad
16 tags, which might load a click tracker or impression pixel instead." *Id.* As Google explains,
17 "Google Marketing Platform advertising products and Google Ad Manager send a cookie to
18 the browser after any impression, click, or other activity that results in a call to our servers." *Id.*

19
20 59. Google also uses cookies in performing analytical functions. As Google
21 explains, "Google Analytics is a platform that collects data from [] websites and apps to create
22

23 ⁸ See, e.g. <https://www.ghostery.com/whotracksme/trackers/doubleclick>.

24 ⁹ See, e.g. About cross-channel remarketing in Search Ads 360 (available at
25 <https://support.google.com/searchads/answer/7189623?hl=en>); About dynamic remarketing for
26 retail (available at [https://support.google.com/google-
27 ads/answer/6099158?hl=en&sjid=1196213575075458908-NC](https://support.google.com/google-ads/answer/6099158?hl=en&sjid=1196213575075458908-NC)).

28 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=1196213575075458908-
NC](https://support.google.com/searchads/answer/2839090?hl=en&sjid=1196213575075458908-NC)); see also Cookies and user identification (available at [https://developers.google.com/tag-
platform/security/concepts/cookies](https://developers.google.com/tag-platform/security/concepts/cookies)).

1 reports that provide insights into [] business[es].”¹¹ “To measure a website ... [one] add[s] a
2 small piece of JavaScript measurement code to each page on [a] site.” *Id.* Then, “[e]very time a
3 user visits a webpage, the tracking code will collect ... information about how that user
4 interacted with the page.” *Id.* Google Analytics enables website owners to “measure when
5 someone loads a page, clicks a link, [] makes a purchase;” “completes a purchase;” “searches
6 [] website or app;” “select content on [] website or app;” “views an item;” and “views their
7 shopping cart.”¹²

8
9 60. Google’s cookies allow it to obtain and store at least the following user data:
10 (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data,
11 (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors,
12 (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and
13 (xii) geolocation data—including whether a user is located in California.¹³
14
15
16
17

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

19 ¹² Set up events (available at
<https://developers.google.com/analytics/devguides/collection/ga4/events>); and Recommended
20 events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>).

21 ¹³ See About the Google Tag (available at
<https://support.google.com/searchads/answer/7550511?hl=en>); How Floodlight Recognizes
22 Users (available at <https://support.google.com/searchads/answer/2903014?hl=en>); How Google
23 Ads tracks website conversions (available at <https://support.google.com/google-ads/answer/7521212>); Google Ads Help, Cookie: Definition (available at
24 <https://support.google.com/google-ads/answer/2407785?hl=en>); About demographic targeting in
25 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
26 Analytics Works (<https://support.google.com/analytics/answer/12159447>); Set up events
27 (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>); and
28 Recommended events (available at <https://support.google.com/analytics/answer/9267735>).

61. 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 <https://www.googleads.g.doubleclick.net>:

The screenshot shows a network request in a browser's developer tools. The request is a GET method to the URL <https://googleads.g.doubleclick.net>. The status is 200. The request details are as follows:

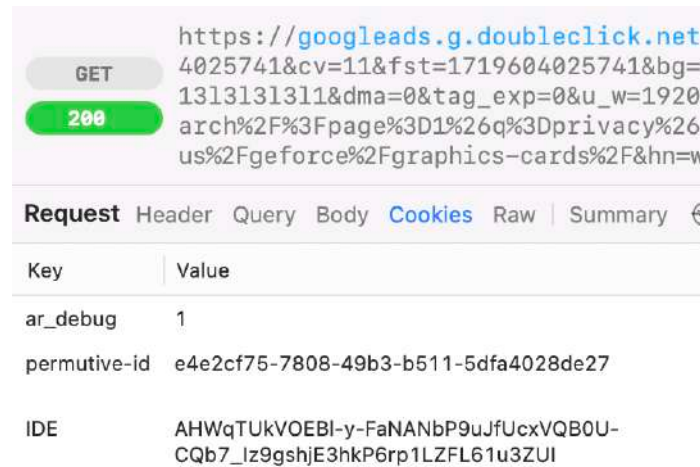
Request	Header	Query	Body	Cookies	Raw	Summary
Key	^ Value					
gtm	45be46q0v885977293za200					
guid	ON					
hn	www.googleadservices.com					
npa	0					
pscdl	noapi					
random	1719604025741					
ref	https://www.nvidia.com/en-us/geforce/graphics-cards/					
rfmt	3					
tag_exp	0					
tiba	Onsite Search: Find What You Seek NVIDIA					
u_h	1080					
u_w	1920					
uaa	x86					
uab	64					
uafvl	Not%2FA)Brand;8.0.0.0 Chromium;126.0.6478.127 Google%20Chrome;126.0.6478.127					
uam						
uamb	0					
uap	Windows					
uapv	10.0.0					
uaw	0					
url	https://www.nvidia.com/en-us/search/?page=1&q=privacy&sort=relevance					
userId	replace with value					

62. 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.

63. The “url” and “tiba” parameters disclose to Google the exact webpage and title that the user was viewing. In this instance, the url discloses the search string the user entered on the website: “privacy.”

64. The “u_h” and “u_w” parameters correspond to the user’s screen height and width.

65. Along with this data, the Google software code that Defendant causes to be stored on and executed by the user’s device causes the following cookies to be sent to Google’s domain:



66. Google documentation confirms that the IDE cookie is used for advertising. Specifically, it is “used to show Google ads on non-Google sites.”¹⁴

67. Defendant identified Google’s IDE cookie as an “Advertising Cookie” used on the Website in the Cookie Policy and described its usage as follows:

IDE	Persistent cookie (expires after 1 year)	Third party (doubleclick)	Used by Google DoubleClick to register and report the website user's actions after viewing or clicking one of the advertiser's ads with the purpose of measuring the efficacy of an ad and to present targeted ads to the user.
-----	--	---------------------------	---

¹⁴ <https://policies.google.com/technologies/cookies?hl=en-UST>

1 68. Further, along with all of this data, the Google software code that Defendant
2 causes to be stored on and executed by the user’s device causes the user’s “user-agent”
3 information to be sent to Google:

4	user-agent	Mozilla/5.0 (Windows NT 10.0;
5		Win64; x64) AppleWebKit/537.36
6		(KHTML, like Gecko) Chrome/
7		126.0.0.0 Safari/537.36

8 69. As discussed above with respect to Facebook, the “user-agent” corresponds to
9 the device and browser that the user has used to access the Website.

10 70. Finally, the data sent to Google contains the user’s IP address—which can be
11 used to determine a user’s geolocation, including whether they are located in California.

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

19 72. Thus, the Google cookies used on the Website cause Google to track users’
20 interactions with advertisements to help advertisers understand how users engage with ads
21 across different websites. Further, the user data collected through the cookie enables the
22 delivery of personalized ads based on user interests and behaviors. For instance, if a user
23 frequently visits travel-related websites, Google will show her more travel-related
24 advertisements. Further, the collected data is used to generate reports for advertisers, helping
25 them assess the performance of their ad campaigns and make data-driven decisions (such as
26 rebranding their products). Further, Google’s advertising platform enables advertisers to
27 retarget marketing, which Google explains allows advertisers to “show previous visitors ads
28 based on products or services they viewed on your website. With messages tailored to your

1 audience, dynamic remarketing helps you build leads and sales by bringing previous visitors
2 back to your website to complete what they started.”¹⁵

3 73. Defendant described the purpose of Google’s cookies as follows in the Website
4 Google Policy:

5
6 This domain is owned by Google Inc. Although Google is primarily known as
7 a search engine, the company provides a diverse range of products and
8 services. Its main source of revenue however is advertising. Google tracks
9 users extensively both through its own products and sites, and the
10 numerous technologies embedded into many millions of websites around
11 the world. It uses the data gathered from most of these services to profile
12 the interests of web users and sell advertising space to organisations
13 based on such interest profiles as well as aligning adverts to the content
14 on the pages where its customer's adverts appear.

15 74. Further, in its “Shared Data Under Measurement Controller-Controller Data
16 Protection Terms,” Google states: “Google can access and analyze the Analytics data
17 customers share with us to better understand online behavior and trends, and improve our
18 products and services—for example, to improve Google search results, detect and remove
19 invalid advertising traffic in Google Ads, and test algorithms and build models that power
20 services like Google Analytics Intelligence that apply machine-learning to surface suggestions
21 and insights for customers based on their analytics data and like Google Ads that applies broad
22 models to improve ads personalization and relevance. These capabilities are critical to the
23 value of the products we deliver to customers today.”¹⁶ Thus, Google can have the capability to
24 use the data it collects for understanding online behavior and trends, machine learning, and
25 improving its own products and services.

26 ¹⁵ Dynamic remarketing for web setup guide (available at <https://support.google.com/google-ads/answer/6077124>).

27 ¹⁶ Shared Data Under Measurement Controller-Controller Data Protection Terms (available at
28 <https://support.google.com/analytics/answer/9024351>).

1 **4. TikTok Cookies**

2 75. Defendant also causes third party cookies to be transmitted to and from Website
3 users’ browsers and devices, even after users elect to “Decline All” cookies including all
4 Performance and Advertising cookies and/or to toggle off “Performance Cookies” and
5 “Advertising Cookies,” to and from the analytics.tiktok.com domain. This domain is associated
6 with TikTok for Business, a suite of tools offered by TikTok, a social media platform owned by
7 ByteDance Ltd., known for short-form video sharing.¹⁷ The TikTok platform is used to create
8 and share videos, and it utilizes cookies for various purposes including assisting brands and
9 marketers to create, manage, and optimize ad campaigns on the platform.¹⁸

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

19 77. These cookies enable TikTok to obtain and store at least the following user data:
20 (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, including
21 *email addresses and phone numbers*; (v) demographic information, (vi) interests and

22 _____
23 ¹⁷ See Our advertising and measurement cookies (available at
24 <https://business.safety.google/adscookies/>).

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

28 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>).

1 preferences, (vii) shopping behaviors, (viii) device information, (ix) session information, (x) user
 2 identifiers, and (xi) geolocation data in the form of the IP address.²⁰

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

```

6 POST 200 https://analytics.tiktok.com/api/v2/pixel/act
7 Request Header Query Body Cookies Raw Summary + PLAIN
8 1 {
9 2   "_inspection": {},
10 3   "action": "Metadata",
11 4   "auto_collected_properties": {
12 5     "content_data": {
13 6       "json_ld": "[]",
14 7       "meta": "{\"title\":\"Graphics Cards by GeForce |
15 8       NVIDIA\", \"meta:description\":\"Explore NVIDIA GeForce
16       graphics cards. RTX 40 series, RTX 30 series, RTX 20
17       series and GTX 16 series.\", \"meta:keywords\":\"geforce
18       graphics cards, GPUs, 40 series, 30 series, 20 series,
19       16 series\"}\",
20       "microdata": "[{\"dimensions\":{\"h\":145,\"w\":258},
21       \"properties\":{\"contentUr\":\"/content/nvidiaGDC/us/
22       en_US/geforce/graphics-cards/_jcr_content/root/
23       responsivegrid/nv_container_1965276325/nv_teaser.
24       coreimg.100.410.jpeg/1694172069214/
25       geforce-rtx-40-series-new.jpeg\"}, \"scopes\": [],
26       \"type\":\"http://schema.org/ImageObject\"},
27       {\"dimensions\":{\"h\":145,\"w\":258}, \"properties\":
28       {\"contentUr\":\"/content/nvidiaGDC/us/en_US/geforce/
29       graphics-cards/_jcr_content/root/responsivegrid/
30       nv_container_1965276325/nv_teaser_copy.coreimg.100.410.
31       jpeg/1694172070105/geforce-rtx-30-series.jpeg\"},
32       \"scopes\": [], \"type\":\"http://schema.org/
33       ImageObject\"}, {\"dimensions\":{\"h\":145,\"w\":258},
34       \"properties\":{\"contentUr\":\"/content/nvidiaGDC/us/
35       en_US/geforce/graphics-cards/_jcr_content/root/
  
```

26 ²⁰ *Id.*; see also TikTok for Business: Enhance Data Postback with the TikTok Pixel
 27 (<https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel?lang=en>);
 28 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>).

```

1 responsivegrid/nv_container_1965276/nv_teaser_copy.
2 coreimg.100.410.jpeg/1694172071136/
3 geforce-gtx-16-series.jpeg\"},\"subscopes\": [],
4 \"type\": \"http://schema.org/ImageObject\"}],
5 9 \"open_graph\": \"{ \"og:site_name\": \"NVIDIA\",
6 \"og:type\": \"Website\", \"og:url\": \"https://www.nvidia.
7 com/en-us/geforce/graphics-cards/\",
8 \"og:title\": \"NVIDIA GeForce Graphics Cards\",
9 \"og:description\": \"GeForce RTX 40, 30, 20 series &
10 GTX 16 series.\", \"og:image\": \"https://www.nvidia.com/
11 content/dam/en-zz/Solutions/geforce/ada/graphics-cards/
12 geforce-ada-4090-web-og-1200x630@2x.jpg\",
13 \"twitter:card\": \"summary_large_image\",
14 \"twitter:site\": \"@NVIDIA\",
15 \"twitter:creator\": \"@NVIDIAGeForce\",
16 \"twitter:title\": \"NVIDIA GeForce Graphics Cards\",
17 \"twitter:url\": \"https://www.nvidia.com/en-us/geforce/
18 graphics-cards/\", \"twitter:description\": \"Explore
19 NVIDIA GeForce graphics cards. RTX 40 series, RTX 30
20 series, RTX 20 series and GTX 16 series.\",
21 \"twitter:image\": \"https://www.nvidia.com/content/dam/
22 en-zz/Solutions/geforce/ada/graphics-cards/
23 geforce-ada-4090-web-og-1200x630@2x.jpg\"}
24 },
25 \"page_trigger\": \"Click\"
26 },
27 \"context\": {
28 \"ad\": {
29 \"jsb_status\": 2,
30 \"sdk_env\": \"external\"
31 },
32 },

```

```
18  ∨  "device": {
19      |  "platform": "pc"
20  },
21  "index": 0,
22  ∨  "library": {
23      |  "name": "pixel.js",
24      |  "version": "2.2.0"
25  },
26  ∨  "page": {
27      |  "load_progress": "2",
28      |  "referrer": "https://www.nvidia.com/en-us/",
29      |  "url": "https://www.nvidia.com/en-us/geforce/
30      |  graphics-cards/"
31  },
31  "pageview_id": "pageId-1719603824484-7435376964767.0.0",
32  ∨  "pixel": {
33      |  "code": "C2V17UTEERJ9G00M6RM0",
34      |  "codes": "C2V17UTEERJ9G00M6RM0|C2DMTL2QV1400ORDIK620",
35      |  "runtime": "1"
36  },
37  "session_id":
38  "b9e54b2f-3586-11ef-9b9c-02001704b732::qPUPoWVZXShfn0PbXsQ
39  n",
38  ∨  "user": {
39      |  "anonymous_id": "D4fWm7WF0wAlgaYuUAr8QYa0dmd"
40  },
41  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
42  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0
43  Safari/537.36",
42  "variation_id": "test_2_single_track"
43  },
```

```

44   "event_id": "",
45   "is_onsite": false,
46   "message_id": "messageId-1719604002911-6453556665542",
47   "properties": {},
48   "signal_diagnostic_labels": {
49     "hashed_email": {
50       "label": "missing"
51     },
52     "hashed_phone": {
53       "label": "missing"
54     },
55     "raw_auto_email": {
56       "label": "missing"
57     },
58     "raw_auto_phone": {
59       "label": "missing"
60     },
61     "raw_email": {
62       "label": "missing"
63     },
64     "raw_phone": {
65       "label": "missing"
66     }
67   },
68   "timestamp": "2024-06-28T19:46:42.911Z"
69 }

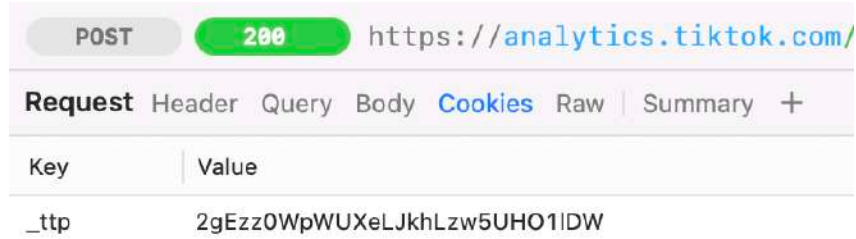
```

79. 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

80. The data discloses extensive information to TikTok regarding the user’s activity on the Website. For example, the “meta” attribute discloses the title of the webpage, as well as keywords relevant to the webpage. The “microdata” attribute discloses the images that the user viewed on the webpage--down to their exact filenames and dimensions. The “page.url” attribute discloses the url of the webpage the user is viewing (here, <https://www.nvidia.com/en-us/geforce/graphics-cards>). The data also discloses the exact time this action occurred, down to the millisecond.

²¹ See, e.g., How to get TikTok session id? (available at <https://gbtimes.com/how-to-get-tiktok-session-id/>).

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’s domain:



82. 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

83. Further, along with all of this data, the TikTok software code that Defendant causes to be stored on and executed by the user’s device causes the user’s “user-agent” information to be sent to TikTok:

user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
------------	---

As discussed above with respect to Facebook, the “user-agent” corresponds to the device and browser that the user has used to access the Website.

84. Finally, the data sent to TikTok includes the user’s IP address—which can be used to determine a user’s geolocation, including whether they are located in California.

85. 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

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>).

1 TikTok advertising campaigns; and performance measurement (i.e., assessing the success of
2 marketing efforts by analyze user responses to ads and content).²³

3 86. Further, TikTok’s Automatic Advanced Matching feature functions as follows:
4 “When a visitor lands on your website and inputs customer information during registration, sign-
5 in, contact, or checkout on a website where you installed your pixel, Automatic Advanced
6 Matching will capture information from those fields. ...TikTok will use hashed information to
7 link event information to people on TikTok. TikTok may use matched events to better attribute
8 events to TikTok ads, optimize advertisers’ future campaigns, and depending on advertisers’ and
9 users’ settings, TikTok may also add people to advertisers’ retargeting or engagement
10 audiences.”²⁴

11 **5. Adobe Cookies**

12 87. Defendant also causes third-party cookies to be transmitted to and from Website
13 users’ browsers and devices, even after users choose to “Decline All” cookies including all
14 Performance and Advertising cookies and/or to toggle off “Performance Cookies” and
15 “Advertising Cookies,” to and from the omtrdc.net domain and the Adobe-owned-and-hosted
16 smetrics.nvidia.com domain. These domains are associated with Adobe Inc.’s Audience
17 Manager, a data management platform, Adobe’s Marketing Cloud, and Adobe’s Experience
18 Cloud Identity Service, a service which provides a universal, persistent ID to identify visitors
19 across all Adobe products. Defendant described the function of Adobe cookies as follows in its
20 Website Cookie Policy: “This domain is owned by Adobe Audience Manager. The main
21 business activity is online profiling for targeted advertising.”

22 88. These cookies are used to assign a unique identifier to each site visitor, which
23 enables Adobe to consistently recognize and track users across different sessions and domains
24 (i.e., cross-site tracking) and collect and synchronize user data to comprehensively observe and
25 _____

26 ²³ See TikTok for Business: Using Cookies with TikTok Pixel
27 (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

28 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>).

1 evaluate user behavior online.²⁵ These cookies enable Adobe to obtain and store at least the
 2 following user data: (i) user identifier; (ii) website interactions; (iii) browsing history; (iv) visit
 3 history; (v) interests and preferences; and (vi) session information.²⁶

4 89. Adobe aggregates this cookie data with other data from multiple channels and
 5 devices, including web analytics, CRM systems, and e-commerce platforms, to create
 6 consumer profiles containing detailed information about a consumer’s behavior, preferences,
 7 and demographics, create audience segments based on shared traits (such as millennials, tech
 8 enthusiasts, etc.), and to enable targeted advertising and marketing analytics.²⁷

9 90. For example, the Adobe software code that Defendant causes to be stored on
 10 and executed by the Website user’s device causes the following query string and cookie data to
 11 be sent to Adobe’s domain, at <https://nvidia.tt.omtrdc.net>:



20 ²⁵ See, e.g., Adobe Experience League: Adobe Analytics cookies (available at
 21 [https://experienceleague.adobe.com/en/docs/core-services/interface/data-](https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/analytics)
 22 [collection/cookies/analytics](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-](https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager)
[collection/cookies/audience-manager](https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager)).

23 ²⁶ See, e.g., Adobe Audience Manager User Guide: Data Collection Components (available at
 24 [https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/system-](https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/system-components/components-data-collection)
[components/components-data-collection](https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/system-components/components-data-collection)).

25 ²⁷ See, e.g., Adobe Audience Manager User Guide: Understanding Calls to the Demdex Domain
 26 (available at [https://experienceleague.adobe.com/en/docs/audience-manager/user-](https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/demdex-calls)
[guide/reference/demdex-calls](https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/demdex-calls)); Adobe Experience Cloud Identity Service overview (available at
 27 <https://experienceleague.adobe.com/en/docs/id-service/using/intro/overview>); Adobe Audience
 28 [Manager Features \(available at https://business.adobe.com/products/audience-](https://business.adobe.com/products/audience-manager/features.html)
[manager/features.html](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-](https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/overview/aam-overview)
[overview](https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/overview/aam-overview)).



91. The “sessionId” key is designed to persist during the entirety of the user’s visit, enabling Adobe to link the user’s pageviews across the website.

92. According to Adobe documentation, the cookie beginning in “s_vi” “[s]tores a unique visitor ID and timestamp.”²⁸ “Each visitor ID is associated with a visitor profile on Adobe servers,” and visitor profiles are set to persist for one year.²⁹

93. Defendant identifies the cookie beginning in “s_vi” as a “Performance Cookie” in its Website Cookie Policy and describes this cookie as follows:

s_vi_cx7Bilodaoblx7Fi	Persistent cookie (expires after 2 years).	Third Party (omtrdc.net)	This domain is owned by Adobe and is used to provide website analytics and optimisation services to clients.
-----------------------	--	--------------------------	--

94. Likewise, the following type of data is sent to Adobe’s domain at https://smetrics.nvidia.com after users have rejected all cookies:

²⁸ <https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/analytics>.

²⁹ *Id.*

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

https://smetrics.nvidia.com/b/ss/nvdaglobalprod/1/JS-8%205%20420&mid=2026576050184864714120673776423215140:tps%3A%2F%2Fwww.nvidia.com%2Fen-us%2Fsearch%2F%3Fpage%3Dv10&v10=search%3Arepeat%3Asuccess%3Aprivacy%20is%important&pe=lnk_o&pev2=search%3Arepeat%3Asuccess%3Apriv

GET 200

Request Header Query Body Cookies Raw Summary +

Key	Value
AQB	1
ndh	1
pf	1
t	28/5/2024 12:48:48 5 420
mid	20265760501848647141206737764232151401
ce	UTF-8
ns	nvda
cdp	2
fpCookieDomainPeriods	2
pageName	nv:search
g	https://www.nvidia.com/en-us/search/?page=1&q=privacy&sort=relevance
cc	USD
events	event10,event21
c10	D=v10
v10	search:repeat:success:privacy is important:nv:search
c20	privacy is important
v20	privacy is important
pe	lnk_o
pev2	search:repeat:success:privacy is important:nv:search
s	1920x1080
c	24
j	1.6
v	N
k	Y
bw	708
bh	953
mcorgid	F207D74D549850760A4C98C6@AdobeOrg
lrt	44
AQE	1

25 95. Along with that data, the following extensive cookie data are sent to Adobe's
26 smetrics.nvidia.com domain:

GET https://smetrics.nvidia.com/b/ss/nvdaglobalprod/1/JS-8%205%20420&mid=2026576050184864714120673776423215146tps%3A%2F%2Fwww.nvidia.com%2Fen-us%2Fsearch%2F%3FpageD%3Dv10&v10=search%3Arepeat%3Asuccess%3Aprivacy%20is%important&pe=lnk_o&pev2=search%3Arepeat%3Asuccess%3Apri

200

Request Header Query Body Cookies Raw Summary +

Key	Value
at_check	true
nvweb_A	cd38578a-f088-4581-9680-46911a61a2f3
s_ecid	MCMID%7C20265760501848647141206737764232151401
AMCVS_F207D74D549850760A4C98C6%40AdobeOrg	1
AMCV_F207D74D549850760A4C98C6%40AdobeOrg	179643557%7CMCMID%7C20265760501848647141206737764232151401%7CMCAID%7CNONE%7CMCOPTOUT-1719610956s%7CNONE%7CvVersion%7C5.5.0
_cs_mk	0.5887334763189811_1719603756629
ak_bmsc	A391E86637DEAF2A3DDB3DFBAF98B206~00000000000000000000000000000000~YAAQzunHF93mMFSQAQAfQBfYBj7cWyau9Ark/h1ZpgkgvhoZnwtg7SyRCsS2z2CRZqKaUaKygYFlyOoGOopLWRzD6A5Oul0opPpwX4k5gXedtF+veNIPxoBecXZ/FNSj+rVJilbHJqXjbJX+TCYZZ++rXkS85TEFhORy7i9n8iDeqv+jk1doYy6P+sfHk9p6mnz7BELvhto8Be8XOsDmx5u+/UrPQqmQyQ/ytnZ45bdVT+b8CJRYEr5mbflwiNSPNowU7qyiehOafd8mnRhtud6TaNgT4vfpIXU7oA+FCyPjpEntkaok5RwWd1CxbkSUjBUGrv6w3QXHOvYMZK0Vooz5GxP07nhJZJ2JhMMRZ2II5ClrJAnLp9l/Et1iIQexRYISOpThNmN2AuVsBoVtHPe8kv4g
_gcl_au	1.1.116464114.1719603758
s_cc	true
_cs_c	0
_hjSession_3655182	eyJpZCI6ImY1NTlhMWVmLTYwNjMtNDkyYi1hYzhlTQ0NTljZTgyNDIzClslmMiOjE3MTk2MDM3NTc3NTkslnMiOjAslnliOjAslnNiljowLCJzci6MZWw2UjUjAslnZzljoxLCJzcCI6MX0=
_vwo_uuid_v2	D8F250E0294AEE4C042C3396214604F39 cc6ef2cb8b04477f62d37d2396d0188c
_biz_uid	09bed99a73f0459cefb5bfc708c4fcd6
_hly_vid	02dd56f0-104e-418e-b9a9-7435093846eb
_vis_opt_s	1%7C
_vis_opt_test_cookie	1
_biz_flagsA	%7B%22Version%22%3A1%2C%22Ecid%22%3A%22-621273206%22%2C%22ViewThrough%22%3A%221%22%2C%22XDomain%22%3A%221%22%2C%22Mkto%22%3A%221%22%22%7D
_fbp	fb.1.1719603758548.124930743920596034
OptanonConsent	isGpcEnabled=0&datestamp=Fri+Jun+28+2024+12%3A43%3A14+GMT-0700+(Pacific+Daylight+Time)&version=202304.1.0&browserGpcFlag=0&isABGlobal=false&hosts=&consentId=30953c2d-2299-40ee-a4d5-36bd8214f436&interactionCount=1&landingPath=https%3A%2F%2Fstore.nvidia.com%2Fen-us%2Fconsumer%2F%3Fpage%3D1%26limit%3D9%26locale%3Den-us%26gpu%3DRTX%25204090%2CRTX%25204080%2CRTX%25204070%2520Ti%2CRTX%25204070%2CRTX%25204060%2520Ti%2CRTX%25204060%2CRTX%25204070%2520SUPER%2CRTX%25204070%2520Ti%2520SUPER%2CRTX%25204080%2520SUPER%26category%3DGPU%2CDESKTOP&groups=C0001%3A1%2CC0002%3A1%2CC0004%3A1%2CC0003%3A1

1 marketing and analytics purposes.³¹ These cookies are used to create an online identification
2 code for the purpose of recognizing users’ devices and tracking their user behavior.

3 98. Defendant identified these cookies as “Advertising Cookies” in the Website
4 Cookie Policy and described its purposes as follows:

5 rlas3	Persistent cookie (expires 6 after 1 year)	Third Party (rlcdn.com)	This cookie is used to deliver advertising more relevant to you and your interests. It is also used to limit the number of times you see an advertisement as well as help measure the effectiveness of the advertising 7 campaign.
---------	---	-------------------------	---

8 99. These cookies enable LiveRamp to obtain and store at least the following user
9 data: browsing history, visit history, website interactions, user input data (such as email address),
10 demographic information, interests and preferences, device information, user identifiers, and
11 geolocation data (including IP addresses), on the Websites. The unique user identifier enables
12 LiveRamp to sell a user’s unique data for use in online and cross-channel advertising (including
13 targeted advertising and email marketing).

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

16 [The website] partner may sell or share personal information collected from you, such as
17 your email, cookies set on your browser, IP address, or information about your browser
18 or operating system, with LiveRamp. LiveRamp uses this information to create an online
19 identification code for the purpose of recognizing your device. This code may be placed
20 in our partners’ cookie and for use in online and cross-channel advertising (including
21 targeted advertising and email marketing), or LiveRamp may connect it to LiveRamp’s
22 own 3rd-party cookie and other identifiers. In addition, by associating an email address
23 with a cookie, LiveRamp and third parties can link your browsing activity across
24 different websites and other applications and services to your specific device associated
25 with the email address, identifying the user behind the device. This means that, even
26 when browsing unrelated sites, your online activity can be connected to you for
27 advertising and other marketing-related purposes, including email marketing and offline
28 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

³¹ See <https://liveramp.com/privacy/service-privacy-policy/#section1a>; *see also* LiveRamp Data Marketplace (available at <https://liveramp.com/data-marketplace/>).

1 enabling interest-based content or targeted advertising throughout your online and offline
 2 experiences (e.g., web, TV [MVPDs], connected TV, mobile applications, email
 3 marketing and other media). These third parties may in turn use this identifier to link
 4 demographic or interest-based information you have provided in your interactions with
 5 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...³²

6 7. Taboola Cookies

7 101. Defendant also causes third party cookies to be transmitted to and from Website
 8 users’ browsers and devices, even after users click or select the “Decline All” button and/or
 9 toggle off “Performance Cookies” and “Advertising Cookies,” to and from the taboola.com
 10 domain.³³ This domain is associated with Taboola, Inc., “one of the world’s leading performance
 11 advertising platforms for the open web. Through our exclusive partnerships with many of the
 12 world’s top websites, we help advertisers engage with over 600 million unique daily active
 13 users.”³⁴ “Taboola’s platform is powered by Deep Learning technology that uses Taboola’s
 14 unique data about people’s interests and information consumption to recommend the right
 15 content to the right person at the right time.”³⁵ Taboola’s technology learns user engagement
 16 patterns by analyzing data it collects using cookies about user “reading preferences, browsing
 17 history, device, location, time of day and more...”³⁶

18 102. Taboola cookies enable it to obtain and store at least the following user data: user
 19 identifiers, browsing history, visit history, website interactions, user input data (such as email
 20 addresses), demographic information (such as gender and age), interests and preferences,
 21 shopping behaviors, device information, referring URLs, session information, user identifiers
 22 (i.e., “cookie IDs”), and/or geolocation data.³⁷ This data allows Defendant to target its

23 ³² Id.

24 ³³ See LiveRamp Product and Service Privacy Notice (available at
<https://liveramp.com/privacy/service-privacy-policy/>).

25 ³⁴ See <https://help.taboola.com/hc/en-us/articles/115006597307-How-Taboola-Works#>.

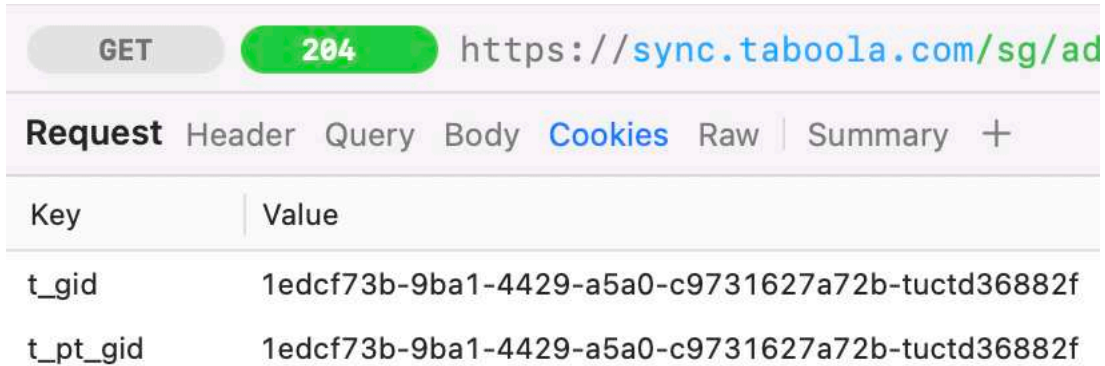
26 ³⁵ Id.

27 ³⁶ Id.

28 ³⁷ 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>).

1 advertising campaigns to users based on user “location, time, browser type, connection type,
2 audience segments, and more.”³⁸

3 103. For example, the Taboola software code that Defendant causes to be stored on and
4 executed by the Websites user’s device causes the following cookie data to be sent to Taboola’s
5 domain, at sync.taboola.com:



Key	Value
t_gid	1edcf73b-9ba1-4429-a5a0-c9731627a72b-tuctd36882f
t_pt_gid	1edcf73b-9ba1-4429-a5a0-c9731627a72b-tuctd36882f

6
7
8
9
10
11
12
13 104. According to Taboola documentation, the “t_gid” cookie “[a]ssigns a unique,
14 User ID that Taboola uses for attribution and reporting purposes, and to tailor recommendations
15 to this specific user based on interactions with an advertiser or publisher.”³⁹ The cookie stays on
16 the consumer’s device and does not expire for an entire year.⁴⁰

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

20 We use User Information for the following purposes: ... **Offering our**
21 **Customers data segments that help target content and advertisements for**
22 **topics, products, and services that may interest you.** A data segment is a
23 grouping of users who share one or more attributes (e.g., travel enthusiasts). We
24 offer a number of data segments, both proprietary and from our data partners, to
25 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

26 ³⁸ See <https://help.taboola.com/hc/en-us/articles/115006597307-How-Taboola-Works#>; see also
27 <https://help.taboola.com/hc/en-us/articles/115001936293-Targeting-Marketplace-Audiences#>.

28 ³⁹ <https://www.taboola.com/policies/cookie-policy>.

⁴⁰ *Id.*

1 affiliations, or Personal Data concerning your sensitive health information, sex
2 life or sexual orientation, or genetic or biometric data). In connection with our
3 Services, our Customers may use these standard health-related segments about
4 non-sensitive conditions such as an inferred interest in health and wellness or over
5 the counter medications. In addition, Taboola offers our Customers standard
6 political-related segments that may indicate general political sentiment, interest in
7 specific political issues, and political party affiliation.⁴¹

8 **8. Salesforce Cookies**

9 106. Defendant also causes data and cookies to be transmitted to and from Website
10 users' browsers and devices, even after users elect to disable all cookies (including
11 "Advertising" cookies), to and from the evergage.com domain, which points to Salesforce's
12 Interaction Studio product. Salesforce describes that product as follows:

13 Interaction Studio enhances the power of Marketing Cloud with
14 expanded real-time personalization. Companies use Interaction
15 Studio to tailor interactions with customers and prospects to
16 increase loyalty, engagement, and conversions. Using real-time
17 cross-channel personalization and machine learning capabilities,
18 Interaction Studio complements Marketing Cloud's robust
19 customer data, audience segmentation, and engagement platform.⁴²

20 107. For instance, Defendant has configured the Nvidia Website to send the
21 following query string and cookie data to be sent to nvidiacorp.us-5.evergage.com, which is
22 hosted by Salesforce:

23
24
25
26
27 ⁴¹ Taboola Privacy Policy (available at <https://www.taboola.com/policies/privacy-policy#information-we-collect-from-users-user-information>) (emphasis in original).

28 ⁴² https://help.salesforce.com/s/articleView?id=sf.mc_isev_interaction_studio.htm&type=5.

1
2
3
4
5
6
7
8
9
10

Key	Value
.anonId	4ef9d671315ab74b
.bv	16
.scv	26
.top	3916
_ak	nvidiacorp
_anon	true
_ds	prod
_r	443384
action	Default Page
channel	Web

11
12
13
14
15
16

Key	Value
AWSALBTGCORS	sTozlv1mrMr0SjPqr0zCRT3stLKYx2XXDGc/t7yl59Atj5Cl6pfuGk/7g6U08mdwvHRvCigBXKhPVQCr4s1KF7IshftJc6btr839ogJtKl2eVhAi0Fqau9a9ZkZaBkeWkv/Q18cpJTppH8t1stEaX2QZjc1GIZ+1+OBGoQFvdj9F09+Ob0M=

17 108. This data informs Salesforce of the exact product that the user was viewing on
18 the Website. The data also includes an “.anonId,” which is an identifier used to uniquely track
19 the user throughout all interactions with the Website.

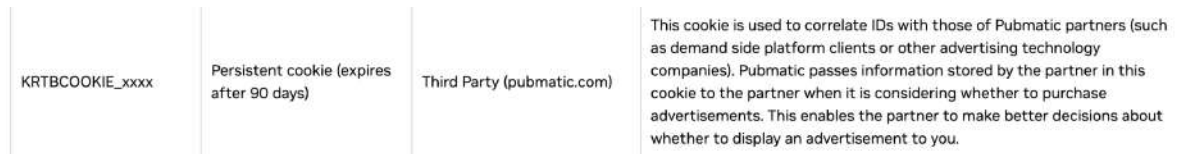
20 109. In addition, Defendant causes the user’s user-agent and IP address information
21 to be sent to Salesforce.

22 **9. Additional Third Party Cookies**

23 110. Defendant also causes third party cookies to be transmitted to and from Website
24 users’ browsers and devices, even after users elect to “Decline All” cookies, including all
25 Performance and Advertising cookies to and from other domains, including pubmatic.com;
26 ib.adnxs.com; px.ads.linkedin.com; analytics.twitter.com; ps.eyeota.net; analytics.yahoo.com;
27
28

1 adroll.com; rubiconproject.com; casalemedia.com; bidswitch.net; 3lift.com; outbrain.com; and
 2 openx.net.

3 111. The **pubmatic.com** domain (and its subdomains) is associated with PubMatic,
 4 Inc., a digital advertising company.⁴³ PubMatic uses pubmatic.com cookies to collect data on
 5 user behavior on websites including user interactions with advertising content.⁴⁴ PubMatic uses
 6 this data to personalize advertising content and track users across the internet.⁴⁵ Defendant
 7 identified pubmatic cookies as “Advertising Cookies” in the Website’s Cookie Policy and
 8 described their purpose as follows:



9
 10
 11
 12 112. The **adnxs.com** domain is associated with AppNexus, owned by Microsoft.
 13 Microsoft uses adnxs.com cookies to collect data on user navigation and behavior on websites,
 14 including information on user preferences and/or interaction with web-campaign content, to
 15 target advertisements.⁴⁶ The cookies include unique identifiers that help Microsoft recognize
 16 users across different websites and sessions.⁴⁷ This allows cookies set from the **adnxs.com**
 17 domain to collect data, including IP address, user demographic information, geographic
 18 location, page views, and interactions with websites.⁴⁸ These cookies also enable Household
 19 Attribution, a feature that enables Microsoft to match ads served on any device to website
 20

21 ⁴³ See www.metrixlab.com.

22 ⁴⁴ See, PubMatic, Inc. Form 10-K for year ending December 31, 2023 (Filed February 28, 2024)
 at 17–18.

23 ⁴⁵ *Id.*

24 ⁴⁶ <https://cookiepedia.co.uk/host/adnxs.com>.

25 ⁴⁷ <https://learn.microsoft.com/pdf?url=https%3A%2F%2Flearn.microsoft.com%2Fen-us%2Fmicrosoft%2Fmonetize%2Ftoc.json>.

26
 27 ⁴⁸ *Id.*; <https://www.microsoft.com/en-us/privacy/privacystatement#mainpersonaldatawecollectmodule>.

1 activity occurring on any device connected to the same network using the same IP address.⁴⁹
2 Further, the cookies enable advertisers to track the effectiveness of campaigns and avoid
3 showing the same ads repeatedly to the same users. Microsoft uses this data to personalize ad
4 content and track users across the internet. Adnxs.com cookies also categorize users into
5 different segments based on their interests, demographics, or behaviors. This segmentation is
6 used to target specific audiences with tailored ads. The data collected by cookies set through
7 the adnxs.com domain has allowed Microsoft to set up a platform in which advertisers can bid
8 for and place advertisements targeted at users based on a variety of demographics, including,
9 among other things, demography, device type, and location.⁵⁰

10 113. The linkedin.com domain is owned by LinkedIn Corporation—a subsidiary of
11 Microsoft Corp. LinkedIn Corporation runs the social media-based business networking
12 platform LinkedIn. Cookies set by the linkedin.com domain are used to target website users
13 with advertising.⁵¹ Defendant identified LinkedIn cookies as “Advertising Cookies” in the
14 Website Cookie Policy and described its usage as follows:

15
16 This domain is owned by LinkedIn, the business networking platform. It
17 typically acts as a third party host where website owners have placed one
18 of its content sharing buttons in their pages, although its content and
19 services can be embedded in other ways. Although such buttons add
20 functionality to the website they are on, cookies are set regardless of
21 whether or not the visitor has an active LinkedIn profile, or agreed to their
22 terms and conditions. For this reason it is classified as a primarily
23 tracking/targeting domain.

24
25 ⁴⁹ <https://learn.microsoft.com/pdf?url=https%3A%2F%2Flearn.microsoft.com%2Fen-us%2Fxandr%2Fmonetize%2Ftoc.json>.

26
27 ⁵⁰ <https://learn.microsoft.com/en-us/xandr/monetize/buy-side-targeting#other-targeting-guidance>.

28 ⁵¹ <https://cookiepedia.co.uk/host/linkedin.com>.

1 114. LinkedIn explains its cookies are used to target users with advertising and
2 measure the performance of such ads.⁵² These cookies assign a unique ID to users' devices,
3 which allows LinkedIn to track users across the internet, and to collect information regarding
4 IP address, operating system, browser information, web browsing activity—including the URL
5 of both the site the users came from before accessing the website with the linkedin.com
6 cookies and the one to which users navigate when they leave the website with the linkedin.com
7 cookies—download and purchase activity, and how users interact with ads.⁵³ Cookies set by
8 the linkedin.com domain are used to target users with advertisements on and off the LinkedIn
9 social media platform.⁵⁴

10 115. The twitter.com domain is associated with X Corp, formerly known as Twitter.
11 X Corp's cookies collect a wide range of user data, including a user's browsing history; IP
12 address; interactions with advertisements; data used to authenticate and secure personal
13 accounts; and reading a device's local storage.⁵⁵ Defendant identified Twitter cookies as
14 "Advertising Cookies" in the Website Cookie Policy that are "primarily used for tracking and
15 targeting." X Corp uses the collected user data to target users with personalized
16 advertisements and content, generate analytics on website interaction, and to conduct
17 unspecified "Research and Development."⁵⁶

18 116. The ps.eyeota.net domain is associated with Eyeota, a subsidiary of Dun &
19 Bradstreet, a "Leading Business Data Analytics" firm.⁵⁷ Eyeota's cookies collect data
20 associated with a user's browser history, as well as anything a visitor interacts with on a
21 particular website page. Eyeota uses the collected data to target users with personalized
22 advertisements, as well as collate data to sell to other businesses to help companies drive
23

24 ⁵² <https://www.linkedin.com/legal/cookie-policy>.

25 ⁵³ *Id.*

26 ⁵⁴ *Id.*

27 ⁵⁵ *See* <https://help.x.com/en/rules-and-policies/x-cookies>.

28 ⁵⁶ *Id.*

⁵⁷ Dun & Bradstreet solutions (available at <https://www.dnb.com/>).

1 growth, manage risk, and strengthen the performance of their business. Defendant identified
2 Eyeota cookies as “Advertising Cookies” in its Website Cookie Policy and described them as
3 “This domain is owned by Eyeota, a global company specialising in audience data to enable
4 targeting of advertising based on visitor profiling.”

5 117. The yahoo.com domain is owned by Yahoo Inc., a technology company that
6 focuses on online media and advertising. Cookies set by the yahoo.com domain are used to
7 target website users with advertising by assigning Website users unique identifiers.⁵⁸ These
8 cookies collect information, such as IP addresses, browser type and settings, operating system,
9 device type, and advertising identifiers from other third parties, including Apple’s ID for
10 Advertising, Apple’s ID for vendors, Google’s Android ID, and Google’s Play Store Ad ID.⁵⁹
11 Cookies are further used to support Yahoo’s targeting of content and advertising and to
12 associate users, devices, and accounts with each other or with those in a similar location, such
13 as in the same household.⁶⁰ Yahoo’s use of a unique identifier with its cookies allows it to
14 track users across the internet and across different devices.⁶¹ The purpose of Yahoo Inc.’s
15 cookies and the data they collect is to track users and target them with advertisements—the
16 sale of which Yahoo uses to generate revenues. Defendant identified Yahoo cookies as
17 “Advertising Cookies” in its Website Cookie Policy and described its main business activity as
18 “Search / Advertising.”

19 118. The adroll.com domain is associated with AdRoll, a digital advertising
20 platform owned by NextRoll, Inc.⁶² AdRoll uses cookies to perform retargeting, a practice that
21 involves tracking users who have previously visited a client’s website and serving them
22

23 ⁵⁸ <https://cookiepedia.co.uk/host/yahoo.com>

24 ⁵⁹ <https://legal.yahoo.com/us/en/yahoo/privacy/topics/cookies/index.html#:~:text=When%20you%20log%20in%20to,or%20device%20you%20are%20using.>

25 ⁶⁰ *Id.*

26 ⁶¹ *Id.*

27 ⁶² See AdRoll Cookies and Opt-Out Options, accessed September 26, 2025,
28 <https://help.adroll.com/hc/en-us/articles/21402369325069-AdRoll-Cookies-and-Opt-Out-Options>

1 personalized advertisements on other websites across the internet.⁶³ These cookies collect data
2 on user browsing activity, website interactions, and cross-device behavior to build user profiles
3 for interest-based advertising campaigns.⁶⁴ AdRoll's technology, through cookies such
4 as `_adroll` and `_adroll_shared`, assigns unique identifiers to users to facilitate this tracking and
5 ad delivery across multiple platforms and devices, enabling a persistent view of a user's
6 activity regardless of whether they are on a desktop or mobile device.⁶⁵

7 119. The **rubiconproject.com** domain is associated with the Rubicon Project, an
8 advertising exchange platform owned by Magnite, Inc.⁶⁶ Rubicon Project operates as a Supply-
9 Side Platform (SSP), enabling website publishers to sell their advertising inventory through
10 real-time bidding auctions. Its cookies are used to assign unique identifiers to users, collect
11 data on their browsing behavior (including IP address, location, and websites visited), and
12 facilitate the exchange of this user data with various ad services.⁶⁷ This process, known as
13 cookie syncing, allows advertisers to identify and bid on ad impressions to target specific users
14 across the web, forming a foundational component of the programmatic advertising
15 ecosystem.⁶⁸

16 120. The **casalemedia.com** domain is associated with Casale Media, a digital
17 advertising technology company that operates as part of an ad exchange network.⁶⁹ Casale
18 Media's cookies are used to collect data about users' website visits and online behavior,
19 including the number of visits, time spent on sites, and pages loaded.⁷⁰ This information is used

20 ⁶³ See Adroll - What Are Cookies? accessed September 26, 2025, <https://www.adroll.com/third-party-cookies/what-are-cookies>.

21 ⁶⁴ See AdRoll Cookies and Opt-Out Options, accessed September 26, 2025,
22 <https://help.adroll.com/hc/en-us/articles/21402369325069-AdRoll-Cookies-and-Opt-Out-Options>.

23 ⁶⁵ See *id.*

24 ⁶⁶ See Platform Cookie Policy - Magnite, accessed September 26, 2025,
<https://www.magnite.com/legal/platform-cookie-policy/>.

25 ⁶⁷ See *id.*; See also User Choice Portal | Manage Your Privacy Preferences with Magnite,
26 accessed September 26, 2025, <https://www.magnite.com/legal/user-choice-portal/>.

27 ⁶⁸ See *id.*

28 ⁶⁹ See <https://www.indexexchange.com/about/>.

⁷⁰ See <https://www.indexexchange.com/privacy/exchange-platform-privacy-policy/>.

1 to build user profiles for the purpose of delivering targeted advertising.⁷¹ The platform enables
 2 advertisers to segment audiences and optimize ad relevance by tracking users across multiple
 3 websites within its network, and its cookies can also be used for functions like frequency
 4 capping to limit the number of times a user is shown the same advertisement.⁷²

5 121. The **bidswitch.net** domain is associated with BidSwitch, Inc., a technology
 6 platform that functions as middleware in the programmatic advertising ecosystem.⁷³
 7 BidSwitch’s cookies are not used to directly serve ads to users, but rather to facilitate the
 8 service of ads between Supply-Side Platforms (SSPs) and Demand-Side Platforms (DSPs).⁷⁴
 9 The cookies store unique user IDs and regulate the synchronization of these IDs across
 10 different advertising services.⁷⁵ This “cookie syncing” is essential for enabling advertisers on
 11 various platforms to recognize a user and participate in real-time bidding auctions for ad space
 12 on publisher websites, effectively acting as a central hub for identity matching in the ad-tech
 13 industry.⁷⁶

14 122. Defendant identified bidswitch cookies as “Advertising Cookies” in its Website
 15 Cookie Policy and described their purpose as follows:

tuid_lu	Persistent cookie (expires after 365 days)	Third Party (bidswitch.net)	This domain is owned by IPONWEB and is used to provide a real time bidding platform for online advertising.
---------	--	-----------------------------	---

16
 17
 18 123. The **3lift.com** domain is associated with TripleLift, Inc., an advertising
 19 technology platform that specializes in programmatic advertising.⁷⁷ TripleLift’s cookies are
 20 used to assign a unique digital identifier (stored in the “TLUID” cookie) to a user’s browser or
 21 device.⁷⁸ This identifier enables the tracking of users across different websites to collect data

22
 23 ⁷¹ *Id.*

⁷² *Id.*

24 ⁷³ See <https://www.bidswitch.com/>

25 ⁷⁴ See <https://www.bidswitch.com/privacy-policy/>.

26 ⁷⁵ *Id.*

⁷⁶ <https://clearcode.cc/blog/what-is-bidswitch/>.

27 ⁷⁷ See <https://triplelift.com/>.

28 ⁷⁸ See <https://triplelift.com/user-rights-policy-and-opt-out/>.

1 for targeted advertising, including interest-based targeting and ad performance measurement.⁷⁹
2 The company also leverages first-party publisher data to create audience segments, positioning
3 this as an addition to traditional third-party cookie tracking in response to industry privacy
4 changes.⁸⁰

5 124. The outbrain.com domain is associated with Outbrain’s advertising services.
6 Outbrain, currently owned and operated by Teads Holding Co., uses cookies to assign a unique
7 user ID to a user’s device to track their content consumption across a network of partner
8 publisher websites.⁸¹ This data, including browsing history and content engagement, is used to
9 build user profiles and interest segments.⁸² These profiles enable Outbrain to serve
10 personalized content and product advertisements, a practice it refers to as “recommendations,”
11 to users on its partner sites. Outbrain’s promoted content is found on over 100,000 websites,
12 and, in 2020, it provided an average of 10 billion content recommendations or deliveries daily
13 for over 20,000 advertisers.⁸³ Further, the cookies perform analytics functions to enable
14 Outbrain to measure and analyze the performance of its services and to ensure that ads are
15 effective and relevant. Outbrain uses machine learning and artificial intelligence to advertise
16 products to consumers that users are likely to find relevant and engaging.⁸⁴

17 125. The openx.net domain is associated with OpenX, a digital advertising
18 technology company that operates a programmatic ad exchange.⁸⁵ Defendant identified
19 openx.net cookies as “Advertising Cookies” in its Cookie Policy. OpenX uses cookies to
20 facilitate the buying and selling of digital advertising. These cookies assign unique online
21 identifiers to users, which are used to collect data across different websites about their online

22 ⁷⁹ See <https://triplelift.com/platform-privacy-policy/>.

23 ⁸⁰ See <https://triplelift.com/resources/case-study/triplelift-audiences-exceed-benchmarks/>

24 ⁸¹ See Privacy FAQ - Outbrain, accessed September 26, 2025,
<https://www.outbrain.com/privacy/privacy-faq/>.

25 ⁸² See Outbrain DSP Cookie Table, accessed September 26, 2025,
<https://www.outbrain.com/privacy/outbrain-dsp-cookie-table/>.

26 ⁸³ See *id.*

27 ⁸⁴ *Id.*

28 ⁸⁵ See <https://www.openx.com/publishers/ad-exchange/>.

1 activity, browsing history, and inferred interests.⁸⁶ This information enables interest-based
2 advertising, allowing advertisers to target specific users with relevant ads. The platform also
3 uses cookies for ad delivery management, such as controlling ad frequency, measuring
4 campaign performance, and syncing user identifiers with other advertising partners.⁸⁷

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

10 **D. The Private Communications Collected are Valuable.**

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

18 128. The Private Communications that the Third Parties track and collect by way of
19 the cookies on the Website are valuable to Defendant as well as the Third Parties. Defendant
20 can use the data to create and analyze the performance of marketing campaigns, website
21 design, product placement, and target specific users or groups of users for advertisements. For
22 instance, if Defendant wanted to market certain of its software or hardware products to
23 consumers in California, Defendant could use the data collected by the Third Parties to monitor
24 the location of users who visit webpages related to specific products, then advertise similar
25 products to those particular users when they visit other webpages. The third-party cookies also
26

27 ⁸⁶ See <https://www.openx.com/privacy-center/ad-exchange-privacy-policy/>.

28 ⁸⁷ See *id.*

1 enable Defendant to target online advertisements to users when they visit *other* websites, even
2 those completely unrelated to Defendant and its products.

3 129. Data about users' browsing history enables Defendant to spot patterns in users'
4 behavior on the Website and their interests in, among other things, Defendant's computer
5 graphics card products. On a broader scale, it enables Defendant to gain an understanding of
6 trends happening across its brands and across the computer graphics card market. All of this
7 helps Defendant further monetize its Website and maximize revenue by collecting and
8 analyzing user data.

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

15 131. Numerous empirical studies quantify the appropriate value measure for personal
16 data. Generally, the value of personal data is measured as either the consumer's willingness to
17 accept compensation to sell her data or the consumer's willingness to pay to protect her
18 information.

19 132. Through its false representations and aiding, agreeing with, employing,
20 permitting, or otherwise enabling the Third Parties to track users' Private Communications on
21 the Website using third-party cookies, Defendant is unjustly enriching itself at the cost of
22 consumer privacy and choice, when the consumer could otherwise have the ability to choose if
23 and how they would monetize their data.

24 **PLAINTIFF'S EXPERIENCES**

25 133. Plaintiff visited the Website to seek and obtain information about NVIDIA's
26 products, while located in California, on multiple occasions during the last four years.

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

1 134. Plaintiff's visits to the Website were consistent with a typical Website user's
2 visits seeking information about Defendant's products. Specifically, Plaintiff is not a consumer
3 advocate, a "tester," or a compliance auditor that visited the Website to test or evaluate
4 Defendant's privacy practices.

5 135. Specifically, Plaintiff searched for company news by typing "news" into the
6 Website search bar. He clicked on some of the Website's "Corporate Blog" posts. Plaintiff also
7 browsed through some of the AI-related products available for sale on the Website, including
8 graphics cards and products related to AI robotics.

9 136. When Plaintiff visited the Website, the Website immediately detected that he
10 was a visitor in California and presented him with Defendant's popup cookie consent banner,
11 which provided the option to select the "Manage Cookies" button. Plaintiff viewed
12 Defendant's representation on the popup cookie consent banner that, "NVIDIA uses cookies to
13 enable and improve the use of the website. Please see our Cookie Policy for more information.
14 You can manage your cookie settings by clicking 'Manage Cookies' or going to the NVIDIA
15 Privacy Center." Accordingly, Plaintiff saw that, rather than choosing to accept such cookies
16 by clicking or selecting the "I Understand" button, users apparently could instead choose to
17 "Manage Cookies" by clicking or selecting the button to do so.

18 137. Consistent with his typical practice in managing or otherwise declining the
19 placement or use of cookies and tracking technologies, Plaintiff selected and clicked the
20 "Manage Cookies" button. In doing so, Plaintiff was then presented with Defendant's Cookie
21 Settings window. There, Defendant further represented that, "NVIDIA websites use cookies to
22 deliver and improve the visitor experience." Defendant, through the Cookie Settings window,
23 represented that the Website used "Performance Cookies[,]" which "[c]ount[] website visits
24 and clicks to understand where people most engage with links[,]" and "Advertising Cookies[,]"
25 which are "[s]et by our advertising partners" and are "used to build a profile of your interests
26 and show you relevant ads on other sites." The window also represented that the Website used
27 "Required Cookies" that are "required for the site to function" and "cannot be turned off."
28

1 Defendant further represented that users, including Plaintiff, could adjust settings or toggles to
2 turn “off” each category of Performance and Advertising cookies, or click or select the
3 “Decline All” button to decline all such cookies, except those “Required” for the Website to
4 function.

5 138. Accordingly, Plaintiff selected and clicked the “Decline All” button, which
6 caused both the popup cookie consent banner and Cookie Settings window to disappear,
7 allowing Plaintiff to browse the Website, which he then proceeded to do. Plaintiff believed that
8 selecting the “Decline All” button on the Cookie Settings window found on the Website would
9 allow him to opt out of, decline, and/or reject “All” cookies and other tracking technologies,
10 except those “Required” for the Website to function (but inclusive of those Performance and
11 Advertising cookies that cause the disclosure of tracking data to third-party performance
12 analytics services and advertising networks and for the purposes of providing performance
13 analytics and advertising services).

14 139. In selecting the “Decline All” button, Plaintiff gave Defendant notice that he did
15 not consent to the use or placement of cookies and tracking technologies while browsing the
16 Website. Further, Plaintiff specifically declined, based on Defendant’s representations, those
17 cookies used to “used to build a profile of your interests and show you relevant ads on other
18 sites[,]” “[c]ount[] website visits and clicks to understand where people most engage with
19 links[,]” and share information with third parties. In reliance on these representations and
20 promises, only then did Plaintiff continue browsing the Website.

21 140. Even before the popup cookie consent banner appeared on the screen,
22 Defendant nonetheless caused cookies and tracking technologies, including those used for
23 advertising and performance analytics, to be placed on Plaintiff’s device and/or transmitted to
24 the Third Parties along with user data, without Plaintiff’s knowledge. Accordingly, the popup
25 cookie consent banner’s and Cookie Settings window’s representations to Plaintiff that he
26 could decline the use and/or placement of “All” cookies and tracking technologies while he
27 browsed the Website were false. Contrary to what Defendant made Plaintiff believe, he did not
28

1 have a choice about whether third-party cookies would be placed on his device and/or
2 transmitted to the Third Parties along with his user data; rather, Defendant had already caused
3 that to happen.

4 141. Then, as Plaintiff continued to browse the Website in reliance on the promises
5 Defendant made in the cookie consent banner and Cookie Settings window, and despite
6 Plaintiff's clear declination of the use and/or placement of such cookies and tracking
7 technologies, Defendant nonetheless continued to cause the placement and/or transmission of
8 cookies along with user data, including those involved in providing advertising and
9 performance analytics from the Third Parties on his device. In doing so, Defendant permitted
10 the Third Parties to track and collect Plaintiff's Private Communications as Plaintiff browsed
11 the Website.

12 142. Defendant's representations that consumers could "Decline All" cookies while
13 Plaintiff and users browsed the Website, or at least those involved in providing advertising and
14 performance analytics, were untrue. Had Plaintiff known this fact, he would not have used the
15 Website. Moreover, Plaintiff reviewed the popup cookie consent banner and Cookie Settings
16 window prior to using the Website. Had Defendant disclosed that it would continue to cause
17 cookies and tracking technologies to be stored on consumers' devices even after they choose to
18 decline "All" such cookies, Plaintiff would have noticed it and would not have used the
19 Website or, at a minimum, he would have interacted with the Website differently.

20 143. Plaintiff continues to desire to browse content featured on the Website. Plaintiff
21 would like to browse websites that do not misrepresent that users can "Decline All" cookies
22 and tracking technologies. If the Website were programmed to honor users' requests to decline
23 "All" cookies and tracking technologies, Plaintiff would likely browse the Website again in the
24 future, but will not do so until then. Plaintiff regularly visits websites that feature content
25 similar to that of the Website. Because Plaintiff does not know how the Website is
26 programmed, which can change over time, and because he does not have the technical
27 knowledge necessary to test whether the Website honors users' requests to "Decline All"
28

1 cookies and tracking technologies, Plaintiff will be unable to rely on Defendant's
2 representations when browsing the Website in the future absent an injunction that prohibits
3 Defendant from making misrepresentations on the Website. The only way to determine what
4 network traffic is sent to third parties when visiting a website is to use a specialized tool such
5 as Chrome Developer Tools. As the name suggests, such tools are designed for use by
6 "developers" (i.e., software developers), whose specialized training enables them to analyze
7 the data underlying the HTTP traffic to determine what data, if any, is being sent to whom.
8 Plaintiff is not a software developer and has not received training with respect to HTTP
9 network calls.

10 **CLASS ALLEGATIONS**

11 144. Plaintiff brings this Class Action Complaint on behalf of himself and a proposed
12 class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal Rules
13 of Civil Procedure. Plaintiff seeks to represent the following group of similarly situated
14 persons, defined as follows:

15 **Class:** All persons who browsed the Website after clicking or selecting the "Decline
16 All" button in the Cookie Settings window and/or after toggling off "Performance
17 Cookies" and "Advertising Cookies" in the Cookie Settings window.

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

21 146. **Numerosity:** Plaintiff does not know the exact size of the Class, but he
22 estimates that it is composed of more than 100 persons. The persons in the Class are so
23 numerous that the joinder of all such persons is impracticable and the disposition of their
24 claims in a class action rather than in individual actions will benefit the parties and the courts.

25 147. **Common Questions Predominate:** This action involves common questions of
26 law and fact to the Class because each class member's claim derives from the same unlawful
27 conduct that led them to believe that Defendant would not cause third-party cookies to be
28

1 placed on their browsers and devices and/or transmitted to third parties along with user data,
2 after Class members chose to “Decline All” cookies and tracking technologies on the Website,
3 nor would Defendant permit third parties to track and collect Class members’ Private
4 Communications as Class members browsed the Website.

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

- 8 a. Whether Defendant’s actions violate California laws invoked herein; and
9 b. Whether Plaintiff and Class members are entitled to damages, restitution,
10 injunctive and other equitable relief, reasonable attorneys’ fees, prejudgment interest and costs
11 of this suit.

12 149. **Typicality:** Plaintiff’s claims are typical of the claims of the other members of
13 the Class because, among other things, Plaintiff, like the other Class members, visited the
14 Website, declined “All” cookies, and had his confidential Private Communications intercepted
15 by the Third Parties.

16 150. **Adequacy of Representation:** Plaintiff will fairly and adequately protect the
17 interests of all Class members because it is in his best interests to prosecute the claims alleged
18 herein to obtain full compensation due to him for the unfair and illegal conduct of which he
19 complains. Plaintiff also has no interests in conflict with, or antagonistic to, the interests of
20 Class members. Plaintiff has retained highly competent and experienced class action attorneys
21 to represent his interests and those of the Class. By prevailing on his claims, Plaintiff will
22 establish Defendant’s liability to all Class members. Plaintiff and his counsel have the
23 necessary financial resources to adequately and vigorously litigate this class action, and
24 Plaintiff and counsel are aware of their fiduciary responsibilities to the Class members and are
25 determined to diligently discharge those duties by vigorously seeking the maximum possible
26 recovery for Class members.
27
28

1 155. Plaintiff and Class members had a reasonable expectation of privacy under the
2 circumstances, as Defendant affirmatively promised users they could “Decline All” cookies
3 and tracking technologies, including all Performance and Advertising cookies, except those
4 cookies “Required” for the Website to function, before proceeding to browse the Website.
5 Plaintiff and other Class members directed their electronic devices to access the Website and,
6 when presented with the popup cookies consent banner and Cookie Settings window on the
7 Website, Plaintiff and Class members declined “All” cookies and reasonably expected that his
8 and their declination of “All” cookies and tracking technologies would be honored. That is, he
9 and they reasonably believed that Defendant would not permit the Third Parties to store and
10 send cookies and/or use other such tracking technologies on their devices while they browsed
11 the Website. Plaintiff and Class members also reasonably expected that, if they declined “All”
12 such cookies and/or tracking technologies, Defendant would not permit the Third Parties to
13 track and collect Plaintiff’s and Class members’ Private Communications, including their
14 browsing history, visit history, website interactions, user input data, demographic information,
15 interests and preferences, shopping behaviors, device information, referring URLs, session
16 information, user identifiers, and/or geolocation data, on the Website.

17 156. Such information is “personal information” under California law, which defines
18 personal information as including “Internet or other electronic network activity information,”
19 such as “browsing history, search history, and information regarding a consumer’s interaction
20 with an internet website, application, or advertisement.” Cal. Civ. Code § 1798.140.

21 157. Defendant, in violation of Plaintiff’s and other Class members’ reasonable
22 expectation of privacy and without their consent, permits the Third Parties to use cookies and
23 other tracking technologies to collect, track, and compile users’ Private Communications,
24 including their browsing history, visit history, website interactions, user input data,
25 demographic information, interests and preferences, shopping behaviors, device information,
26 referring URLs, session information, user identifiers, and/or geolocation data—including
27 whether a user is located in California. The data that Defendant allowed third parties to collect
28

1 enables the Third Parties to (and they in fact do), *inter alia*, create consumer profiles
2 containing detailed information about a consumer’s behavior, preferences, and demographics;
3 create audience segments based on shared traits (such as Millennials, Californians, tech
4 enthusiasts, etc.); and perform targeted advertising and marketing analytics. Further, the Third
5 Parties share user data and/or the user profiles to unknown parties to further their financial
6 gain. The consumer profiles are and can be used to further invade Plaintiff’s and users’
7 privacy, by allowing third parties to learn intimate details of their lives, and target them for
8 advertising and other purposes, as described herein, thereby harming them through the
9 abrogation of their autonomy and their ability to control dissemination and use of information
10 about them.

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

15 159. Defendant’s intrusion into Plaintiff’s privacy was also highly offensive to a
16 reasonable person.

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

23 161. Plaintiff and Class members have been damaged by Defendant’s invasion of
24 their privacy and are entitled to just compensation, including monetary damages.

25 162. Plaintiff and Class members seeks appropriate relief for that injury, including
26 but not limited to, damages that will compensate them for the harm to their privacy interests as
27
28

1 well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's
2 and Class members' privacy.

3 163. Plaintiff and Class members seek punitive damages because Defendant's
4 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and
5 Class members and made in conscious disregard of Plaintiff's and Class members' rights and
6 Plaintiff's and Class members' declination of the Website's use of "All" cookies, including all
7 Performance and Advertising cookies, except those cookies "Required" for the Website to
8 function. Punitive damages are warranted to deter Defendant from engaging in future
9 misconduct.

10 **Second Cause of Action: Intrusion Upon Seclusion**

11 164. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

12 165. To assert a claim for intrusion upon seclusion, Plaintiff must plead (i) that
13 Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiff had
14 a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a
15 reasonable person.

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

25 167. The Third Parties' tracking and collecting of Plaintiff's and Class member's
26 Private Communications on the Website using third-party cookies that Defendant caused to be
27 stored on users' devices—and to be transmitted to Third Parties—was not authorized by
28

1 Plaintiff and Class members, and, in fact, those Website users specifically chose to “Decline
2 All” cookies, including all Performance and Advertising cookies, except those cookies
3 “Required” for the Website to function.

4 168. Plaintiff and the Class members had an objectively reasonable expectation of
5 privacy surrounding his and their Private Communications on the Website based on
6 Defendant’s promise that users could “Decline All” cookies, as well as state criminal and civil
7 laws designed to protect individual privacy.

8 169. Defendant’s intentional intrusion into Plaintiff’s and other users’ Private
9 Communications would be highly offensive to a reasonable person given that Defendant
10 represented that Website users could “Decline All” cookies when, in fact, Defendant caused
11 such third-party cookies to be stored on consumers’ devices and browsers, and to be
12 transmitted to third parties, even when consumers declined all such cookies. Indeed, Plaintiff
13 and Class members reasonably expected, based on Defendant’s false representations, that when
14 he and they declined “All” cookies and tracking technologies, including all Performance and
15 Advertising cookies, except those cookies “Required” for the Website to function, Defendant
16 would not cause such third-party cookies to be stored on his and their devices or permit the
17 Third Parties to obtain their Private Communications on the Website, including their browsing
18 history, visit history, website interactions, user input data, demographic information, interests
19 and preferences, shopping behaviors, device information, referring URLs, session information,
20 user identifiers, and/or geolocation data—including whether a user is located in California.

21 170. Defendant’s conduct was intentional and intruded on Plaintiff’s and users’
22 Private Communications on the Website.

23 171. Plaintiff and Class members have been damaged by Defendant’s invasion of
24 their privacy and are entitled to just compensation, including monetary damages.

25 172. Plaintiff and Class members seeks appropriate relief for that injury, including
26 but not limited to, damages that will compensate them for the harm to their privacy interests as
27
28

1 well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff’s
2 and Class members’ privacy.

3 173. Plaintiff and Class members seek punitive damages because Defendant’s
4 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and
5 Class members and made in conscious disregard of Plaintiff’s and Class members’ rights and
6 Plaintiff’s and Class members’ declination of the Website’s use of “All” cookies, including all
7 Performance and Advertising cookies, except those cookies “Required” for the Website to
8 function. Punitive damages are warranted to deter Defendant from engaging in future
9 misconduct.

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

12 174. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

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

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

25 176. The California Supreme Court has repeatedly stated an “express objective” of
26 CIPA is to “protect a person placing or receiving a call from a situation where the person on
27 the other end of the line permits an outsider to tap his telephone or listen in on the call.” *Ribas*
28 *v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

177. Further, as the California Supreme Court has held, in explaining the legislative
purpose behind CIPA:

While one who imparts private information risks the betrayal of his confidence by
the other party, a substantial distinction has been recognized between the
secondhand repetition of the contents of a conversation and *its simultaneous*

1 *dissemination to an unannounced second auditor, whether that auditor be a*
2 *person or mechanical device.*

3 As one commentator has noted, such secret monitoring denies the speaker an
4 important aspect of privacy of communication—the right to control the nature
5 and extent of the firsthand dissemination of his statements.

6 *Ribas*, 38 Cal. 3d at 360-61 (emphasis supplied; internal citations omitted).

7 178. CIPA § 631(a) imposes liability for “distinct and mutually independent patterns
8 of conduct.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish
9 liability under § 631(a), Plaintiff need only establish that Defendant, “by means of any
10 machine, instrument, contrivance, or in any other manner,” did **any** of the following:

11 [i] Intentionally taps, or makes any unauthorized connection, whether physically,
12 electrically, acoustically, inductively or otherwise, with any telegraph or telephone
13 wire, line, cable, or instrument, including the wire, line, cable, or instrument of any
14 internal telephonic communication system;

15 [ii] Willfully and without the consent of all parties to the communication, or in any
16 unauthorized manner, reads or attempts to read or learn the contents or meaning of any
17 message, report, or communication while the same is in transit or passing over any
18 wire, line or cable or is being sent from or received at any place within this state;

19 [iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in
20 any way, any information so obtained

21 Cal. Penal Code § 631(a).

22 179. CIPA § 631(a) also penalizes those who [iv] “aid[], agree[] with, employ[], or
23 conspire[] with any person” who conducts the aforementioned wiretapping, or those who
24 “permit” the wiretapping.

25 180. Defendant is a “person” within the meaning of California Penal Code § 631.

26 181. Section 631(a) is not limited to phone lines, but also applies to “new
27 technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL
28 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be
construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v.*
Google, Inc., 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic
communications”); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31,
2022) (“Though written in terms of wiretapping, Section 631(a) applies to Internet
communications.”).

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

6 183. Each of the Third Parties is a “separate legal entity that offers [a] ‘software-as-
7 a-service’ and not merely a passive device.” *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D.
8 Cal. 2021). Further, the Third Parties had the capability to use the wiretapped information for
9 their own purposes and, as alleged above, they did in fact use the wiretapped information for
10 their own business purposes. Accordingly, the Third Parties were third parties to any
11 communication between Plaintiff and Class members, on the one hand, and Defendant, on the
12 other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal.
13 2023).

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

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

25 186. At all relevant times, by their cookies and corresponding software code, the
26 Third Parties willfully and without the consent of all parties to the communication, or in any
27 unauthorized manner, read, attempted to read, and/or learned the contents or meaning of
28

1 electronic communications of Plaintiff and Class members, on the one hand, and Defendant, on
2 the other, while the electronic communications were in transit or were being sent from or
3 received at any place within California.

4 187. The Private Communications of Plaintiff and Class members, on the one hand,
5 and Defendant, on the other, that the Third Parties automatically intercepted directly
6 communicates the Website user’s affirmative decisions, actions, choices, preferences, and
7 activities, which constitute the “contents” of electronic communications, including their
8 browsing history, visit history, website interactions, user input data, demographic information,
9 interests and preferences, shopping behaviors, device information, referring URLs, session
10 information, user identifiers, and/or geolocation data—including whether a user is located in
11 California.

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

15 189. Plaintiff and Class members did not provide their prior consent to the Third
16 Parties’ intentional access, interception, reading, learning, recording, collection, and usage of
17 Plaintiff’s and Class members’ electronic communications. Nor did Plaintiff and Class
18 members provide their prior consent to Defendant aiding, agreeing with, employing,
19 permitting, or otherwise enabling the Third Parties’ conduct. On the contrary, Plaintiff and
20 Class members expressly declined to allow Third Parties’ cookies and tracking technologies to
21 access, intercept, read, learn, record, collect, and use Plaintiff’s and Class members’ electronic
22 communications by choosing to “Decline All” cookies in the Cookie Settings window.

23 190. The wiretapping of Plaintiff and Class members occurred in California, where
24 Plaintiff and Class members accessed the Website and where the Third Parties—as caused by
25 Defendant—routed Plaintiff’s and Class members’ electronic communications to Third Parties’
26 servers. Among other things, the cookies, as well as the software code responsible for placing
27 the cookies and transmitting them and other Private Communications to the Third Parties,
28

1 resided on Plaintiff's California-located device. In particular, the user's California-based
2 device, after downloading the software code from the Third Parties' servers, (i) stored the code
3 onto the user's disk; (ii) converted the code into machine-executable format; and (iii) executed
4 the code, causing the transmission of data (including cookie data) to and from the Third
5 Parties.

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

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

15 193. Unless enjoined, Defendant will continue to commit the illegal acts alleged
16 herein including, but not limited to, permitting third parties to access, intercept, read, learn,
17 record, collect, and use Plaintiff's and Class members' electronic Private Communications with
18 Defendant. Plaintiff, Class members, and the general public continue to be at risk because
19 Plaintiff, Class members, and the general public frequently use the internet to search for
20 information and content related to computer hardware and software products, such as the
21 computer graphics cards Defendant manufactures and sells. Plaintiff, Class members, and the
22 general public continue to desire to use the internet for that purpose. Plaintiff, Class members,
23 and the general public have no practical way to know if his and their request to "Decline All"
24 cookies and tracking technologies will be honored and/or whether Defendant will permit third
25 parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members'
26 electronic Private Communications with Defendant. Further, Defendant has already permitted
27 the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class
28

1 members' electronic Private Communications with Defendant and will continue to do so unless
2 and until enjoined.

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

5 194. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

6 195. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to
7 638, includes the following statement of purpose:

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

14 196. California Penal Code Section 638.51(a) proscribes any “person” from
15 “install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court
16 order.”

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

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

26 199. At all relevant times, Defendant caused the Third Parties' cookies and the
27 corresponding software code—which are pen registers—to be placed on Plaintiff's and Class
28 members' browsers and devices, and/or to be used to transmit Plaintiff's and Class members'
IP address and user-agent information. *See Greenley v. Kochava*, 2023 WL 4833466, at *15-16

1 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11
2 (N.D. Cal. Oct. 21, 2024).

3 200. Some of the information collected by the Third Parties' cookies and the
4 corresponding software, including IP addresses and user-agent information, does not constitute
5 the content of Plaintiff's and the Class members' electronic communications with the Website.
6 *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). ("IP addresses constitute
7 addressing information and do not necessarily reveal any more about the underlying contents
8 of communication...") (cleaned up).

9 201. Plaintiff and Class members did not provide their prior consent to Defendant's
10 use of third-party cookies and the corresponding software. On the contrary, Plaintiff and the
11 Class members informed Defendant that they did not consent to the Website's use of third-
12 party cookies by clicking or selecting the "Decline All" button in the Cookie Settings window
13 and/or by toggling off "Performance Cookies" and "Advertising Cookies" in the Cookie
14 Settings window.

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

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

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

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

23 205. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

24 206. Defendant fraudulently and deceptively informed Plaintiff and Class members
25 that he and they could "Decline All" cookies, including all Performance and Advertising
26 cookies, except those cookies "Required" for the Website to function.

1 207. However, despite Defendant’s representations otherwise, Defendant caused
2 third-party cookies and software code to be stored on consumers’ devices, and to be
3 transmitted to the Third Parties alongside Private Communications, even after users clicked or
4 selected the “Decline All” button in the Cookie Settings window and/or by toggled off
5 “Performance Cookies” and “Advertising Cookies” in the Cookie Settings window. These
6 cookies and corresponding software code allowed the Third Parties to access, intercept, read,
7 learn, record, collect, and use Plaintiff’s and Class members’ Private Communications, even
8 when consumers had previously chosen to decline all cookies.

9 208. These misrepresentations and omissions were known exclusively to, and
10 actively concealed by Defendant, not reasonably known to Plaintiff and Class members, and
11 material at the time they were made. Defendant knew, or should have known, how the Website
12 functioned, including the Third Party’s resources it installed on the Website and the third-party
13 cookies in use on the Website, through testing the Website, evaluating its performance metrics
14 by means of its accounts with the Third Parties, or otherwise, and knew, or should have known,
15 that the Website’s programming allowed the third-party cookies to be placed on users’—
16 including Plaintiff’s—browsers and devices and/or transmitted to the Third Parties along with
17 users’ Private Communications even after users attempted to “Decline All” cookies, including
18 all Performance and Advertising cookies, except those cookies “Required” for the Website to
19 function, which Defendant promised its users they could do. Defendant’s misrepresentations
20 and omissions concerned material facts that were essential to the analysis undertaken by
21 Plaintiff and Class members as to whether to use the Website. In misleading Plaintiff and Class
22 members and not so informing him and them, Defendant breached its duty to Plaintiff and
23 Class members. Defendant also gained financially from, and as a result of, its breach.

24 209. Plaintiff and Class members relied to their detriment on Defendant’s
25 misrepresentations and fraudulent omissions.

26 210. Plaintiff and Class members have suffered an injury-in-fact, including the loss
27 of money and/or property, as a result of Defendant’s unfair, deceptive, and/or unlawful
28

1 practices, including the unauthorized interception of his and their Private Communications,
2 including their browsing history, visit history, website interactions, user input data,
3 demographic information, interests and preferences, shopping behaviors, device information,
4 referring URLs, session information, user identifiers, and/or geolocation data, which have
5 value as demonstrated by the use and sale of consumers' browsing activity, as alleged above.
6 Plaintiff and Class members have also suffered harm in the form of diminution of the value of
7 his and their private and personally identifiable information and communications.

8 211. Defendant's actions caused damage to and loss of Plaintiff's and Class
9 members' property right to control the dissemination and use of their personal information and
10 communications.

11 212. Defendant's representation that consumers could "Decline All" cookies
12 (including those Advertising cookies "used to build a profile of your interests and show you
13 relevant ads on other sites" and those Performance cookies used to "[c]ount[] website visits
14 and clicks to understand where people most engage with links") if they clicked or selected the
15 "Decline All" cookies button and/or by toggled off "Performance Cookies" and "Advertising
16 Cookies" in the Cookie Settings window was untrue. Again, had Plaintiff and Class members
17 known these facts, they would not have used the Website. Moreover, Plaintiff and Class
18 members reviewed the popup cookie consent banner and Cookie Settings window prior to their
19 interactions with the Website. Had Defendant disclosed that it caused third-party non-
20 "Required" cookies to be stored on Website visitors' devices that relate to advertising and
21 performance analytics, and/or share information with third parties, even after they choose to
22 decline all such cookies, Plaintiff and Class members would have noticed it and would not
23 have interacted with the Website.

24 213. By and through such fraud, deceit, misrepresentations and/or omissions,
25 Defendant intended to induce Plaintiff and Class members to alter their positions to their
26 detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiff and Class
27 members to, without limitation, use the Website under the mistaken belief that Defendant
28

1 would not permit third parties to obtain users' Private Communications when consumers chose
2 to decline all cookies, including all Performance and Advertising cookies, except those cookies
3 "Required" for the Website to function. As a result, Plaintiff and the Class provided more
4 personal data than they would have otherwise.

5 214. Plaintiff and Class members justifiably and reasonably relied on Defendant's
6 misrepresentations and omissions, and, accordingly, were damaged by Defendant's conduct.

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

10 216. Plaintiff and Class members seek punitive damages because Defendant's
11 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and
12 Class members and made in conscious disregard of Plaintiff's and Class members' rights and
13 Plaintiff's and Class members' declination of the Website's use of all non-required cookies.
14 Punitive damages are warranted to deter Defendant from engaging in future misconduct.

15 **Sixth Cause of Action: Unjust Enrichment**

16 217. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

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

19 219. Defendant was unjustly enriched as a result of its wrongful conduct, including
20 through its misrepresentation that users could "Decline All" cookies, including all Performance
21 and Advertising cookies, except those cookies "Required" for the Website to function, and by
22 permitting the Third Parties to store and transmit cookies on Plaintiff's and Class members'
23 devices and browsers, which permitted the Third Parties to track and collect users' Private
24 Communications, including their browsing history, visit history, website interactions, user
25 input data, demographic information, interests and preferences, shopping behaviors, device
26 information, referring URLs, session information, user identifiers, and/or geolocation data,
27 even after Class members declined "All" such cookies.
28

1 220. Plaintiff and Class members' Private Communications have conferred an
2 economic benefit on Defendant.

3 221. Defendant has been unjustly enriched at the expense of Plaintiff and Class
4 members, and Defendant has unjustly retained the benefits of its unlawful and wrongful
5 conduct.

6 222. Defendant appreciated, recognized, and chose to accept the monetary benefits
7 that Plaintiff and Class members conferred onto Defendant at his and their detriment. These
8 benefits were the expected result of Defendant acting in its pecuniary interest at the expense of
9 Plaintiff and Class members.

10 223. It would be unjust for Defendant to retain the value of Plaintiff's and Class
11 members' property and any profits earned thereon.

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

15 225. Plaintiff and Class members are entitled to restitution of the benefits Defendant
16 unjustly retained and/or any amounts necessary to return Plaintiff and Class members to the
17 position he and they occupied prior to having his and their Private Communications tracked
18 and collected by the Third Parties.

19 226. Plaintiff pleads this claim separately, as well as in the alternative, to his other
20 claims, as without such claims Plaintiff would have no adequate legal remedy.

21 **PRAYER FOR RELIEF**

22 **WHEREFORE**, reserving all rights, Plaintiff, on behalf of himself and the Class
23 members, respectfully requests judgment against Defendant as follows:

24 A. Certification of the proposed Class, including appointment of Plaintiff's counsel
25 as class counsel;

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

4 C. An award of punitive damages;

5 D. An award of nominal damages;

6 E. An order for full restitution;

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

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

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

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

13 Dated: October 24, 2025

14 **GUTRIDE SAFIER LLP**

15 */s/ Seth A. Safier/s/*

16 Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

17 Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

18 Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

19 100 Pine Street, Suite 1250

San Francisco, CA 94111

20 Telephone: (415) 639-9090

Facsimile: (415) 449-6469

21 *Attorneys for Plaintiff*

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [NVIDIA Disregards Website Visitors' Cookie Preferences, Class Action Lawsuit Claims](#)
