

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ESTRELLA EUGENIO and REVITAL
YOGEV, individuals, on behalf of themselves,
the general public, and those similarly situated,

Plaintiffs,

v.

PREMIUM BRANDS OPCO LLC,

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	INTRODUCTION	1
2	THE PARTIES.....	3
3	JURISDICTION AND VENUE	3
4	FRAUDULENT CONCEALMENT AND TOLLING.....	4
5	SUBSTANTIVE ALLEGATIONS	5
6	A. Defendant Programmed the Websites to Include Third-Party Resources that	
7	Utilize Cookie Based Tracking Technologies.	5
8	B. Defendant Falsely Informed Users That They Could Reject the Websites’ Use of	
9	Cookies.	11
10	C. The Private Communications Intercepted and Collected Through Third-Party	
11	Cookies on Defendant’s Websites.	22
12	1. The Websites Cause the Interception of the Contents of Communications.	22
13	2. Google Cookies.....	25
14	3. TikTok Cookies.	32
15	4. Adobe Cookies.....	37
16	5. Additional Third-Party Cookies.....	48
17	D. The Third Parties Intercept User Communications While in Transit.	52
18	E. The Signaling and Addressing Information Intercepted by the Third Parties.	55
19	F. The Private Communications Collected are Valuable.	56
20	PLAINTIFFS’ EXPERIENCES	57
21	CLASS ALLEGATIONS	64
22	CAUSES OF ACTION.....	66
23	First Cause of Action: Invasion of Privacy.....	66
24	Second Cause of Action: Intrusion Upon Seclusion.....	69
25	Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy	
26	Act (California Penal Code § 631).....	71
27	Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of	
28	Privacy Act (California Penal Code § 638.51)	74
	Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation.....	76

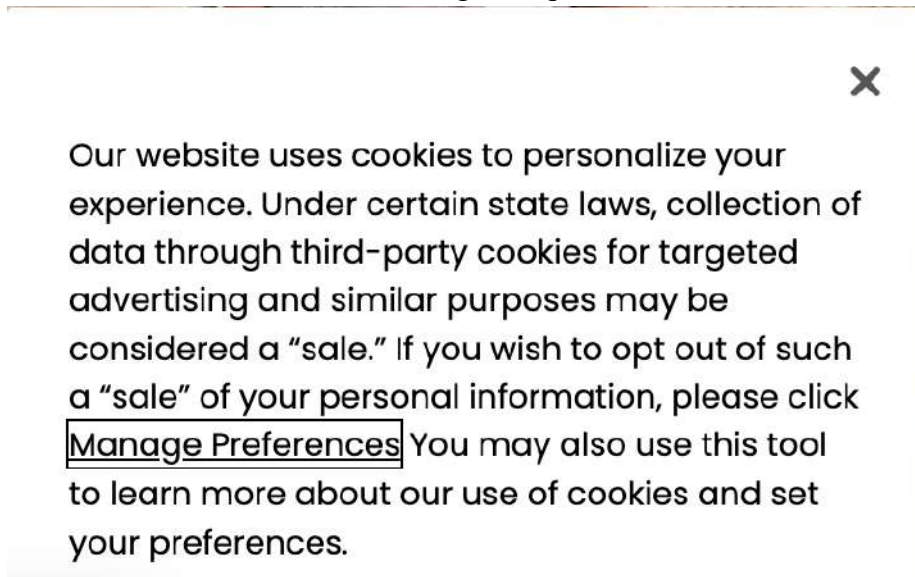
Sixth Cause of Action: Unjust Enrichment.....78

PRAYER FOR RELIEF79

Plaintiffs Estrella Eugenio and Revital Yogev (“Plaintiffs”) bring this action on behalf of themselves, the general public, and all others similarly situated against Premium Brands Opco LLC (“Defendant” or “Loft”). Plaintiffs’ allegations against Defendant are based on information and belief and the investigation of Plaintiffs’ counsel, except for allegations specifically pertaining to Plaintiffs, which are based on their personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns egregious violations of consumer privacy and breach of consumer trust in violation of California law. When consumers visit Defendant’s ecommerce websites (www.loft.com, the “Loft Website”; www.anntaylor.com, the “Ann Taylor Website”; and, www.lanebryant.com, the “Lane Bryant Website”; each a “Website” and, collectively, the “Websites”), Defendant displays to them a popup cookie consent banner, which is identical on each of the Websites. Defendant’s cookie banners disclose that the Websites use cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendant assures visitors that they can opt out of cookies by clicking “Manage Preferences” as shown in the following example screenshot from the Loft Website:



2. Like most internet websites, Defendant designed the Websites to include resources and programming scripts from third parties that cause those parties to place cookies and other similar tracking technologies on visitors’ browsers and devices and/or transmit cookies along with user data. Unlike many other websites, however, Defendant affirmatively represented

1 that users could browse the Websites without being tracked, followed, or targeted by third-party
2 data brokers and advertisers. Those representations were false.

3 3. Even after users elect to opt out of all cookies, including Advertising and
4 Functional cookies, other than those cookies “Strictly Necessary” for the operation of the
5 Websites, Defendant nonetheless caused multiple third parties—including Google LLC
6 (DoubleClick and Google Analytics), TikTok USDS Joint Venture LLC (TikTok), Adobe Inc.
7 (dpm.demdex.net), Salesforce, Inc. (p.cquotient.com), Snap Inc. (SnapChat), Everest
8 Technologies, Inc. (cm.everesttech.net), Pinterest, Inc., MNTN, Inc. (mountain.com), OpenX
9 Technologies, Inc. (openx.net), The Trade Desk, Inc. (adsrvr.org), and more (the “Third
10 Parties”)—to place and/or transmit cookies that track users’ website browsing activities and
11 intercepted their private communications on the Websites.

12 4. Contrary to users’ express choice to opt out of cookies and tracking technologies
13 on the Websites, Defendant caused cookies, including the Third Parties’ cookies, to be sent to
14 Plaintiffs and other visitors’ browsers, stored on their devices, and transmitted to the Third
15 Parties along with user data. These cookies permitted the Third Parties to track and collect data
16 in real time regarding the Websites’ visitors’ behaviors and communications, including their
17 browsing history, visit history, website interactions, user input data, demographic information,
18 interests and preferences, shopping behaviors, device information, referring URLs, session
19 information, user identifiers, and/or geolocation data—including whether a user is located in
20 California.

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

27 6. This type of tracking and data sharing is exactly what the Websites’ visitors
28 sought to avoid when they adjusted the toggle switches on the Websites’ Cookie Preference

Center to opt out of all non-strictly necessary cookies (including Advertising and Functional cookies). Defendant falsely told its Websites' users that it respected their privacy choices and would refrain from tracking and data sharing when users opt out of or rejected cookies. Despite receiving clear notice of users' lack of consent, Defendant ignored those choices and violated state statutes and tort duties owed to Plaintiffs and those similarly situated Website users.

THE PARTIES

7. Plaintiff Estrella is, and was at all relevant times, an individual and resident of San Jose, California. Plaintiff Eugenio intends to remain in California and makes her permanent home there.

8. Plaintiff Revital Yogev is, and was at all relevant times, an individual and resident of North Hollywood, California. Plaintiff Yogev intends to remain in California and makes her permanent home there.

9. Defendant Premium Brands Opco LLC is an Ohio limited liability company with its principal place of business in New York, New York.

JURISDICTION AND VENUE

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

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

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

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

1 California, including within this District.

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

3 **FRAUDULENT CONCEALMENT AND TOLLING**

4 15. The delayed discovery rule applies to Plaintiffs' claims. Plaintiffs were unaware
5 that, despite rejecting all non-strictly necessary cookies (including Advertising and Functional
6 cookies) on the Websites, Defendant nonetheless caused third-party cookies to be sent to their
7 browsers, stored on their devices, and transmitted to the Third Parties along with their private
8 user data. Plaintiffs could not reasonably have discovered this conduct at the time of their visits
9 to the Websites because it occurred through hidden, technical processes not visible to ordinary
10 users. Nothing about Plaintiffs' experiences on the Websites would have alerted a reasonable
11 user that their selections were not being honored. Plaintiffs lacked the technical expertise and
12 specialized tools necessary to determine whether the Websites honored their opt-out selections
13 or instead continued transmitting their data notwithstanding those selections, and they did not
14 discover Defendant's conduct until a later investigation revealed it.

15 16. On or about June 5, 2024, Defendant was notified by Plaintiffs' counsel that it
16 was engaging in the conduct alleged herein, including causing third-party cookies and
17 corresponding user data to be stored on consumers' devices and transmitted to third parties
18 despite users' rejection of all non-strictly necessary cookies (including Advertising and
19 Functional cookies) and the selling of user information. Despite this notice, Defendant did not
20 disclose this conduct to users.

21 17. Despite exercising reasonable diligence, Plaintiffs were unaware of Defendant's
22 conduct because Defendant affirmatively represented that users could opt out of all non-strictly
23 necessary cookies, including Advertising and Functional cookies, while simultaneously
24 concealing that such tracking would occur regardless of users' selections. This combination of
25 misrepresentation and omission prevented Plaintiffs from discovering their claims earlier.
26 Defendant is not prejudiced by the timing of this action, as it has long been on notice of the
27 conduct at issue, including through the June 5, 2024 demand letter describing substantially
28

1 similar claims. These circumstances, including Defendant's concealment and misleading
2 representations, warrant tolling of the statute of limitations.

3 **SUBSTANTIVE ALLEGATIONS**

4 **A. Defendant Programmed the Websites to Include Third-Party Resources that Utilize** 5 **Cookie Based Tracking Technologies.**

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

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

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

24 21. Defendant voluntarily integrated "third-party resources" from the Third Parties
25 into its Websites' programming. "Third-party resources" refer to tools, content or services
26 provided by third parties, such as analytics tools, advertising networks, or payment processors,
27 that a website developer utilizes by embedding scripts, styles, media, or application
28 programming interface (API) into the website's code. Defendant's use of the third-party

resources on the Websites is done so pursuant to agreements between Defendant and those Third Parties.

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

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

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

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

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

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

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

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

10 27. Defendant owns, operates, markets, and manages several women's apparel and
11 retail brands, including Loft, Ann Taylor, and Lane Bryant, through both brick-and-mortar retail
12 stores and the Websites. The Websites allow visitors to, among other things, browse products,
13 review pricing and promotions, search for store locations, and purchase apparel and related
14 products online. As they interact with the Websites—including by entering information into
15 forms, searching for products, selecting sizes or styles, adding items to shopping carts, clicking
16 links, and navigating webpages—Website users communicate Private Communications to
17 Defendant, including their browsing history, visit history, website interactions, user input data,
18 demographic information, interests and preferences, shopping behaviors, device information,
19 referring URLs, session information, user identifiers, and/or geolocation data—including
20 whether a user is located in California.

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

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

Information That is Collected Automatically

We may collect information automatically when you visit and use our Channels ("Device ID / Interaction Information"). For example, we automatically collect your information when you open or respond to our emails, contact customer service or use support tools, visit any page that displays our ads or content, connect or link to any Channel via social networking sites, post comments to online communities or provide information to our service providers, including our advertising and business partners. The following are examples of how we automatically collect information through the Sites:

Browsing and Device Information: We automatically collect some information and data about your computer and mobile devices when you visit our Channels. For example, we will collect your IP address, web browser software, and information about referring websites. We also may collect information about your online activity, such as merchandise viewed and purchases made, as well as general location data that helps us to tailor the version of the Channel that you see in order to enhance your shopping experience.

Cookies: Cookies are small data files stored on your computer's web browser. These technologies can store a unique identifier for a device to allow a certain Internet site to recognize the device whenever the device is used to visit the site. These technologies may be used for many purposes by us and our third-party service providers, such as automatically collecting Device ID / Interaction Information, enabling features, remembering your preferences, and providing you with targeted advertising elsewhere online. If you do not want to accept cookies, you can block them by adjusting the settings on your Internet browser, however, some features of the website may not function if you block all cookies. You may also elect to limit the use of cookies in connection with targeted advertising, as described in the Third Party Advertising and Analytics section below.

Pixel Tags: We use 'pixel tags' (small graphic images also called web beacons or clear gifs) or similar technologies to track information in the aggregate about your use of the Sites like the web pages you view, the links you click, and the time you spend on a page. We use this information to monitor the effectiveness of our advertising and marketing campaigns so we can learn how to best deliver your customer experience. We also use pixels to track our email campaigns to determine whether recipients opened the email and what links they clicked on from the email.

Embedded Scripts: An embedded script is programming code that is designed to collect information about your interactions with the Sites, such as the links you click on. The code is temporarily downloaded onto your device from our server or a third-party service provider, is active only while you are connected to a Site, and is deactivated or deleted thereafter.

Analytics tools and aggregate data: The Sites use analytics tools, such as Google Analytics and Adobe Analytics, web analytics services provided by Google, Inc. and Adobe, Inc., respectively. Google Analytics and Adobe Analytics use cookies to help the Sites analyze how you use the Sites. The information generated by the cookie about your use of the Sites (including your

IP address) will be transmitted to and stored by Google and Adobe, respectively, in aggregate form. Google and Adobe may use this aggregated information in order to evaluate use of the sites, compile reports on Sites activity and other services relating to Sites activity and usage.

THIRD PARTY ADVERTISING AND ANALYTICS / PRIVACY CONTROLS

We may work with network advertisers, ad agencies, analytics service providers, and other vendors to serve our advertisements on our Channels and third-party websites, apps, and elsewhere online, to provide us with data regarding use of and traffic on the Channels (including without limitation the pages viewed and the actions users take when visiting the Channels), and the effectiveness of our advertisements. For example, if you click on an advertisement for Premium Brands, our service provider(s) may be able to tell us the advertisement you clicked on and where you were viewing the advertisement. The advertisements you see may be served by us or one or more third parties, who may use data about your activities on the Channels, and other websites and services you visit across the various devices you use, to provide you targeted content and advertising. Our service providers may collect certain data about your visits to and activity on the Channels and other websites and services and may use this data to target advertising to you.

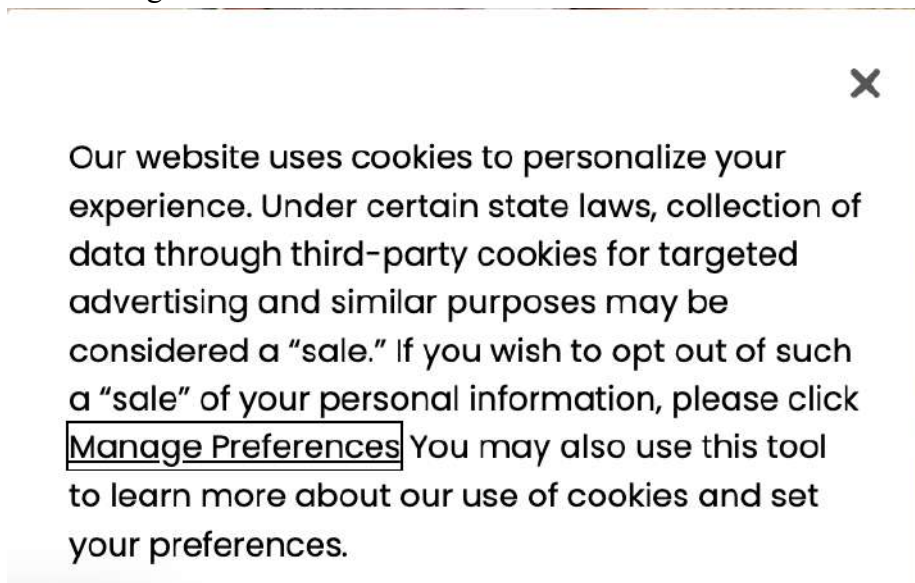
These third parties may set and access their own tracking technologies on your device (including without limitation cookies and web beacons) and may otherwise collect or have access to information about you (such as Device ID/Interaction Information). Some of these parties may collect personal data over time when you visit the Channels or other online websites and services. Cookies and web beacons, including without limitation those set by third-party network advertisers, may be used to (among other things): target advertisements, prevent you from seeing the same advertisements too many times, and conduct research regarding the usefulness of certain advertisements to you. We may share certain data, such as device identifiers, Device ID/Interaction Information, hashed information, records of transactions you conduct on our Channels or offline, and other types of de-identified or pseudonymized data with third-party advertising companies, analytics providers, and other vendors for advertising and analytics purposes. In addition, we and our third-party service providers may use this data to perform matching with third-party cookies to provide targeted online marketing. If you would like to opt-out of third-party advertising and analytics, there are a variety of tools available to you:

- **Cookie Opt-Out Tools:** To disable sharing through cookies set on our site by third parties for advertising and analytics purposes, please adjust your settings by using our Cookie Management Tool. Residents of some states have additional rights to opt-out of the sharing or processing of their personal information for purposes of targeted advertising, as described in the Jurisdiction-Specific Rights section below.¹

¹ Premium Brands Privacy Policy (Last Updated as of April 15, 2026) (available at <https://www.loft.com/loft-privacy/>) (the "Privacy Policy").

B. Defendant Falsely Informed Users That They Could Reject the Websites’ Use of Cookies.

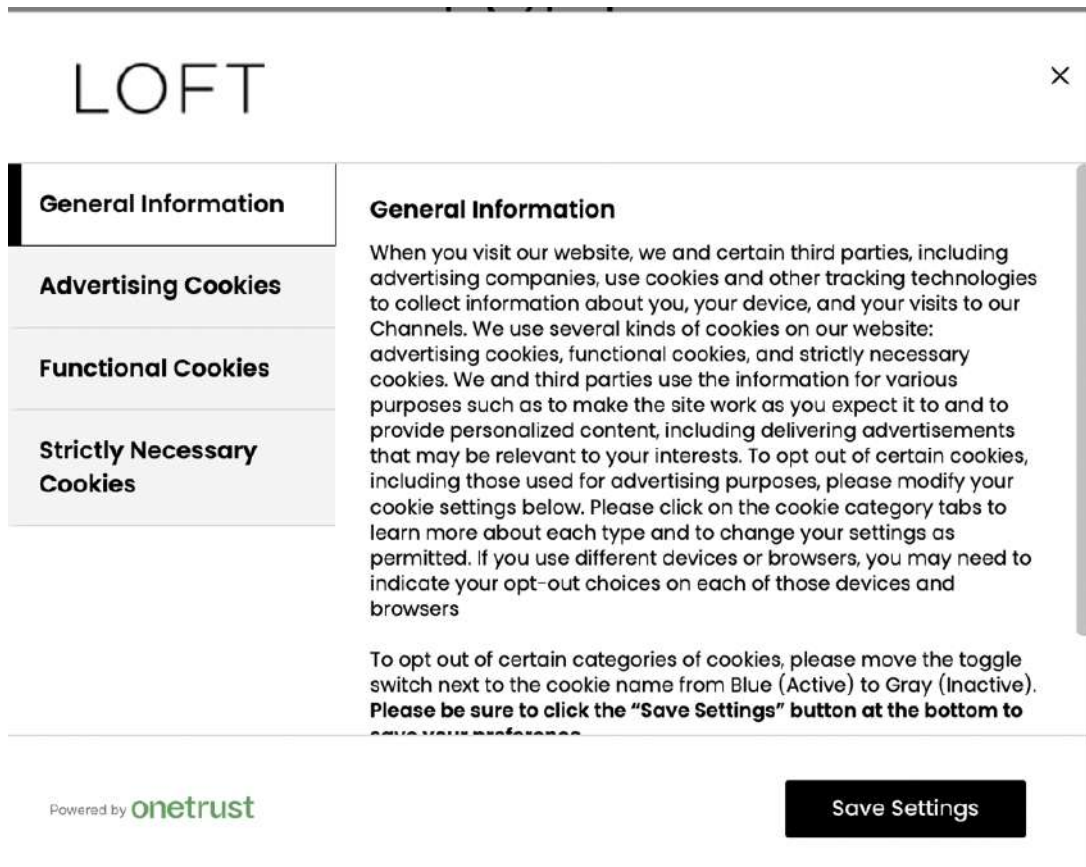
30. When Plaintiffs and other consumers in California visited the Websites, the Websites immediately displayed to them a popup cookie consent banner, which was identical on each of the Websites. As shown in the example screenshot below, the cookie consent banner stated, “Our website uses cookies to personalize your experience. Under certain state laws, collection of data through third-party cookies for targeted advertising and similar purposes may be considered a ‘sale.’ If you wish to opt out of such a ‘sale’ of your personal information, please click Manage Preferences[.] You may also use this tool to learn more about our use of cookies and set your preferences.” The text “Manage Preferences” was a hyperlink that users could click, as shown in the following screenshot from the Loft Website:



31. Plaintiffs and other Website users who clicked or selected the “Manage Preferences” link were then presented with Defendant’s Cookie Preference Center (which was substantially similar in form and content on each of the Websites), where Defendant represented its Websites’ users could “opt out of certain cookies, including those used for advertising purposes,” by moving “the toggle switch next to the cookie name from Blue (Active) to Gray (Inactive).”

32. Defendant further represented that its Websites’ users could opt out of or reject all “Advertising Cookies,” which it defined as those that “collect data from visitors through

cookies in order to personalize [the user] experience, including to serve [users] targeted content and ads[.]” and that users could also opt out of or reject all “Functional Cookies,” which are those used to “provide enhanced functionality” and “may be set by [Defendant] or by third party providers[.]” Defendant advised users that they could not opt out of or reject “Strictly Necessary Cookies,” which are “necessary for the website to function and cannot be switched off[.]” These representations are as shown in the following screenshots from the Loft Website:



LOFT

Advertising Cookies

Functional Cookies

Strictly Necessary Cookies

advertising companies, use cookies and other tracking technologies to collect information about you, your device, and your visits to our Channels. We use several kinds of cookies on our website: advertising cookies, functional cookies, and strictly necessary cookies. We and third parties use the information for various purposes such as to make the site work as you expect it to and to provide personalized content, including delivering advertisements that may be relevant to your interests. To opt out of certain cookies, including those used for advertising purposes, please modify your cookie settings below. Please click on the cookie category tabs to learn more about each type and to change your settings as permitted. If you use different devices or browsers, you may need to indicate your opt-out choices on each of those devices and browsers

To opt out of certain categories of cookies, please move the toggle switch next to the cookie name from Blue (Active) to Gray (Inactive). **Please be sure to click the "Save Settings" button at the bottom to save your preference.**

Please refer to our Privacy Policy [here](#) at any time for more information on our practices.

Powered by onetrust

Save Settings

LOFT

General Information

Advertising Cookies

Functional Cookies

Strictly Necessary Cookies

Advertising Cookies

Targeting/Advertising Cookies/Do Not Sell or Share for Cross-Context Advertising We and our third party advertising, analytics, social media, and similar partners may collect data from visitors through cookies in order to personalize your experience, including to serve you targeted content and ads.

Under certain circumstances, the collection of personal information through these cookies may be considered "sales", "sharing", or "targeted advertising" under applicable laws. To opt out of selling/sharing/targeting advertising click [here](#).

Powered by onetrust

Save Settings

Allow All Cookies

LOFT

×

General Information

Advertising Cookies

Functional Cookies

Strictly Necessary Cookies

Functional Cookies

These cookies enable the website to provide enhanced functionality and user experience (for example, to remember choices you make when using our site). They may be set by us or by third party providers whose services we have added to our pages.

☐

Powered by onetrust

Save Settings

Allow All Cookies

LOFT

×

General Information

Advertising Cookies

Functional Cookies

Strictly Necessary Cookies

Strictly Necessary Cookies

Always Active

These cookies are necessary for the website to function and cannot be switched off in our systems.

Powered by onetrust

Save Settings

Allow All Cookies

1 33. Users who adjusted the toggle switches to the inactive position next to all
2 categories of cookies, including all Advertising and Functional cookies, thereby indicating their
3 choice and/or agreement to opt out of or reject all cookies and tracking technologies in use on the
4 Websites, other than those strictly necessary for the Websites to function, could then continue to
5 browse the Websites after clicking or selecting the “Save Settings” button, as the popup cookie
6 consent banner and Cookie Preference Center disappeared.

7 34. Defendant’s popup cookie consent banner and Cookie Preference Center led
8 Plaintiff, and all those users of the Websites similarly situated, to believe that they declined or
9 rejected all cookies and tracking technologies, especially those that used to “collect data from
10 visitors through cookies in order to personalize [the user] experience, including to serve [users]
11 targeted content and ads.” The Websites’ banner and Cookie Preference Center further reasonably
12 led Plaintiffs and those users of the Websites similarly situated to believe that Defendant would
13 not allow third parties, through cookies, to access their Private Communications with the
14 Websites, including their browsing history, visit history, website interactions, user input data,
15 demographic information, interests and preferences, shopping behaviors, device information,
16 referring URLs, session information, user identifiers, and/or geolocation data, upon adjusting the
17 toggle switches on the Cookie Preference Center to opt out of or reject all categories of cookies,
18 including all Advertising and Functional cookies, other than those cookies strictly necessary for
19 the Websites to function.

20 35. Defendant’s representations, however, were false. In truth, Defendant did not
21 abide by Plaintiffs’ or other users’ wishes. When Plaintiffs and other users of Defendant’s
22 Websites adjusted the available toggle switches to the inactive position on the cookies preferences
23 window, they provided notice to Defendant that they did not consent to the placement or
24 transmission of third-party cookies that would allow those parties to obtain their Private
25 Communications with the Websites.

26 36. Nevertheless, even after receiving that notice, Defendant caused the Third-Party
27 tracking cookies to be placed on the Websites’ users’ browsers and devices and/or transmitted to
28 the Third Parties along with user data.

1 37. In particular, when users adjusted the available toggle switches to the inactive
2 position on the cookies preferences window, Defendant nonetheless continued to cause the Third
3 Parties' cookies to be placed on users' devices and/or transmitted to the Third Parties along with
4 user data, enabling them to collect user data in real time that discloses Websites' visitors' Private
5 Communications, including browsing history, visit history, website interactions, user input data,
6 demographic information, interests and preferences, shopping behaviors, device information,
7 referring URLs, session information, user identifiers, and/or geolocation data. In other words,
8 even when consumers like Plaintiffs tried to protect their privacy by rejecting cookies, Defendant
9 failed to prevent cookies from being transmitted to Third Parties, enabling them to track user
10 behavior and communications.

11 38. Some aspects of the operations of the Third-Party cookies on the Websites can be
12 observed using specialized tools that log incoming and outgoing network transmissions. The
13 following screenshots, obtained using one such tool, show examples of Third-Party cookies being
14 transmitted from a Website user's device and browser to Third Parties even after the user adjusted
15 the available toggle switches to the inactive position on the Cookie Preference Center and
16 confirmed these choices by clicking or selecting the "Save Settings" button.

17
18
19
20 **[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]**
21
22
23
24
25
26
27
28

a. From the Loft Website:

catl000013/767282.html?priceSort=DES

Name	Method	Status	Domain	Cookies
1069304232/?random=1717395567893&...	GET	200	www.google.com	6
anchor?ar=1&k=6Ld5V4AUAAAAIoJc8g...	GET	200	www.google.com	6
anchor?ar=1&k=6Ld5V4AUAAAAIoJc8g...	GET	200	www.google.com	6
ibs:dpid=411&dpuuid=ZfykaQAAWbUFCw...	GET	200	dpm.demdex.net	3
id?d_visid_ver=5.5.0&d_fieldgroup=AAM...	GET	200	dpm.demdex.net	3
1069304232/?random=1717395567893&c...	GET	200	td.doubleclick.net	2
1069304232/?random=1717395570767&c...	GET	200	googleads.g.doubleclick.net	2
1069304232/?random=1717395567893&...	GET	200	googleads.g.doubleclick.net	2
dd?d_uuid=33422539022878840694432...	GET	302	cm.everesttech.net	2
dest5.html?d_nsid=0	GET	200	anntaylor.demdex.net	2
1069304232/?random=1717395570767&c...	GET	200	td.doubleclick.net	2
p	POST	200	tr.snapchat.com	1
p	POST	200	tr.snapchat.com	1
act	POST	200	analytics.tiktok.com	1
p	POST	200	tr.snapchat.com	1
act	POST	200	analytics.tiktok.com	1
act	POST	200	analytics.tiktok.com	1
collect?v=2&tid=G-E84NBG6G00>m=4...	POST	204	www.google-analytics.com	1
p	POST	200	tr.snapchat.com	1
collect?v=2&tid=G-E84NBG6G00>m=4...	POST	204	www.google-analytics.com	1
collect?v=1&_v=j101&a=184396954&t=pa...	GET	200	www.google-analytics.com	1
pebble?tia=bjbk-Loft&activityType=viewC...	GET	200	p.cquotient.com	1
collect?v=1&_v=j101&a=769715985&t=pa...	POST	200	www.google-analytics.com	1
graphql?disableSetCookie=true	OPTIO...	204	www.paypal.com	0
hashes	OPTIO...	200	rl.quantummetric.com	0
messaging?locale=en-US&client_id=b673...	OPTIO...	204	js.klarna.com	0
index.html?showButtons=false&showBack...	GET	(cancele...	osm.klarnaservices.com	0
index.html?showButtons=false&showBack...	GET	200	osm.klarnaservices.com	0
view-placement	OPTIO...	200	metrics.kmsmep.com	0
view-placement	OPTIO...	200	metrics.kmsmep.com	0
config	OPTIO...	200	brands.kmsmep.com	0
upstream-messaging-events?disableSetC...	OPTIO...	204	api.paypal.com	0
consentreceipts	OPTIO...	200	privacyportal.onetrust.com	0
style	OPTIO...	200	brands.kmsmep.com	0
index.html?showButtons=false&showBack...	GET	200	osm.klarnaservices.com	0
main.js	GET	200	osm.klarnaservices.com	0
fonts.css	GET	200	x.klarnacdn.net	0
main.js	GET	200	osm.klarnaservices.com	0
fonts.css	GET	200	x.klarnacdn.net	0

b. From the Ann Taylor Website:

clothing/tops-and-blouses/cata000010/839252.html?dwvar_839252_color=5139&priceSort=DES

Name	Method	Status	Domain	Cookies
collect?v=2&tid=G-KLH5L175DT&_ng=1>...	POST	204	analytics.google.com	6
collect?v=2&tid=G-KLH5L175DT&_ng=1>...	POST	204	analytics.google.com	6
1069304232/?random=1717395815285&cv...	GET	200	www.google.com	6
1069304232/?random=1717395812568&cv...	GET	200	www.google.com	6
ibs:dpid=411&dpuuid=ZfykaQAAWbUFCwBN...	GET	200	dpm.demdex.net	3
id?d_visid_ver=5.5.0&d_fieldgroup=AAM&d...	GET	200	dpm.demdex.net	3
1069304232?random=1717395815285&cv...	GET	200	td.doubleclick.net	2
1069304232?random=1717395812568&cv...	GET	200	td.doubleclick.net	2
1069304232/?random=1717395815285&cv...	GET	200	googleads.g.doubleclick.net	2
1069304232/?random=1717395812568&cv...	GET	200	googleads.g.doubleclick.net	2
dd?d_uuid=334225390228788406944322...	GET	302	cm.everesttech.net	2
dest5.html?d_nsid=0	GET	200	anntaylor.demdex.net	2
pixel	POST	200	analytics.tiktok.com	1
collect?v=1&_v=j101&a=1351015122&t=page...	GET	200	www.google-analytics.com	1
pebble?tla=bj bk-AnnTaylor&activityType=vie...	GET	200	p.cquotient.com	1
pebble?tla=bj bk-AnnTaylor&activityType=cli...	GET	200	p.cquotient.com	1
collect?v=1&_v=j101&a=855180631&t=page...	GET	200	www.google-analytics.com	1
pebble?tla=bj bk-AnnTaylor&activityType=vie...	GET	200	p.cquotient.com	1
messaging?locale=en-US&client_id=964cc1...	OPTIO...	204	js.klarna.com	0
wpt.json	OPTIO...	204	cdn0.forter.com	0
index.html?showButtons=false&showBackgr...	GET	(canceled)	osm.klarnaservices.com	0
index.html	GET	200	www.paypalobjects.com	0
hashes	OPTIO...	200	rl.quantummetric.com	0
consentreceipts	OPTIO...	200	privacyportal.onetrust.com	0
noop.js	GET	200	www.paypalobjects.com	0
interstitial_view?bespokeId=payment-calcul...	POST	204	evt-eu.klarnaservices.com	0
messaging?locale=en-US&client_id=964cc1...	GET + ...	200	js.klarna.com	0
main.js	GET	200	osm.klarnaservices.com	0
fonts.css	GET	200	x.klarnacdn.net	0
smart-credit-modal-v2@1.64.4.js	GET	200	www.paypalobjects.com	0
js?client-id=AaJCfS3urw4s9mNlwBu68sK78...	GET	200	www.paypal.com	0
PayPalOpen-Regular.woff2	GET	200	www.paypalobjects.com	0
839259_018572_ALT1	GET	200	anninc.scene7.com	0
839259_018572	GET	200	anninc.scene7.com	0
839259_018572_MKTG1	GET	200	anninc.scene7.com	0
835058_018572_ALT2	GET	200	anninc.scene7.com	0
835058_018572_ALT1	GET	200	anninc.scene7.com	0
835058_018572	GET	200	anninc.scene7.com	0
835058_018572_MKTG1	GET	200	anninc.scene7.com	0

c. From the Lane Bryant Website:

relaxed-v-neck-knit-woven-top/prd-406295.html?dwvar_406295_color=0000111028&catid=cat10001

Name	Method	Status	Domain	Cookies
anchor?ar=1&k=6LcKBs4kAAAAIH0EYXNt...	GET	200	www.google.com	6
anchor?ar=1&k=6LcKBs4kAAAAIH0EYXNt...	GET	200	www.google.com	6
1002073794/?random=519347481&cv=11&f...	GET	302	www.google.com	6
1002073794/?random=1108844965&cv=11...	GET	302	www.google.com	6
ig-membership?ntk=e7rd_Zs3decg9yjrqaOa...	GET	200	us.creativecdn.com	5
v2?type=json	POST	200	us.creativecdn.com	5
v3/?event=pagevisit&tid=2615532646242&...	GET	200	ct.pinterest.com	3
v3/?tid=2615532646242&pd=%7B%22pin_...	GET	200	ct.pinterest.com	3
user/?event=pagevisit&tid=2615532646242...	GET	200	ct.pinterest.com	3
user/?tid=2615532646242&pd=%7B%22pin...	GET	200	ct.pinterest.com	3
1002073794/?random=1717395972820&cv=...	GET	200	td.doubleclick.net	2
1002073794/?random=1717395974358&cv=...	GET	(canceled)	td.doubleclick.net	2
1002073794/?random=1717395972789&cv=...	GET	200	td.doubleclick.net	2
st?ga_tracking_id=G-1111111&ga_client_id=...	GET	200	px.mountain.com	2
1002073794/?random=519347481&cv=11&f...	GET	302	googleads.g.doubleclick.net	2
1002073794/?random=1108844965&cv=11...	GET	302	googleads.g.doubleclick.net	2
cm?id=b9f5c7de-85f6-48cc-ba86-351b90...	GET	302	us-u.openx.net	2
sd?id=537141727&val=1807266205152206...	GET	200	us-u.openx.net	2
up_loader.1.1.0.js	GET	200	js.adsrvr.org	2
1002073794/?random=1717395972812&cv=...	GET	200	td.doubleclick.net	2
1002073794/?random=1717395974375&cv=...	GET	(canceled)	td.doubleclick.net	2
p	POST	200	tr.snapchat.com	1
p	POST	200	tr.snapchat.com	1
p	POST	200	tr.snapchat.com	1
act	POST	200	analytics.tiktok.com	1
act	POST	200	analytics.tiktok.com	1
p	POST	200	tr.snapchat.com	1
act	POST	200	analytics.tiktok.com	1
sv.js?sv_cid=3611_04124&sv_origin=lanebry...	GET	200	track.sv.rkdms.com	1
1002073794/?random=1717395974375&cv=...	GET	(unknown)	www.googleadservices.com	1
1002073794/?random=1717395974358&cv=...	GET	(unknown)	www.googleadservices.com	1
collect?v=2&tid=G-9YEFHRYN96>m=45j...	POST	204	www.google-analytics.com	1
collect?v=2&tid=G-NGJM6H11P0>m=45je...	POST	204	www.google-analytics.com	1
idsync?proto=rtbhouse&ssp_uid=PgMHtnkq...	GET	200	tg.socdm.com	1
i.match?p=b12&redirect=https%3A%2F%2F...	GET	302	a.tribalfusion.com	1
visitor?%7B%22tagKey%22%3A%22144631...	GET	302	302 Found ion.com	1
1002073794/?random=1717395972820&cv=...	GET	200	www.googleadservices.com	1
1002073794/?random=1717395972812&cv=...	GET	200	www.googleadservices.com	1
spx?dxver=4.0.0&shaid=36924&tdr=https%...	GET	200	dx.mountain.com	1

Name	Method	Status	Domain	Cookies
sv.js?sv_cid=3611_04124&sv_origin=lanebry...	GET	200	track.sv.rkdms.com	
config	OPTIO...	200	brands.kmsmep.com	
view-placement	OPTIO...	200	metrics.kmsmep.com	
wpt.json	OPTIO...	204	cdn0.forter.com	
style	OPTIO...	200	brands.kmsmep.com	
messaging?placement_key=credit-promotio...	OPTIO...	204	js.klarna.com	
messaging?placement_key=credit-promotio...	OPTIO...	204	js.klarna.com	
rum	POST	204	lanebryant.quiq-api.com	
conversation-starter-storage-3.1.1176-ad8e...	GET	200	static.quiq-cdn.com	
vef91dfe02fce4ee0ad053f6de4f175db1715...	GET	200	static.cloudflareinsights.com	
noop.js	GET	200	www.paypalobjects.com	

39. 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 Websites at <https://www.loft.com>, <https://www.anntaylor.com>, and <https://www.lanebryant.com>, respectively. The screenshots depict only network traffic occurring *after* the user rejected all categories of cookies, including all Advertising and Functional cookies, using the toggle switches available in the cookies preferences window. As shown above, despite the user’s rejection of all cookies, the user’s interactions with the Websites resulted in the user’s browser making a large number of GET and POST HTTP requests to third party web domains like google.com, analytics.tiktok.com, dpm.demdex.net; and others. As further shown in the right-hand column of the screenshots, the user’s browser sent cookies along with those HTTP requests to the third parties. These screenshots demonstrate that Defendant caused third-party cookie data and users’ Private Communications to be transmitted to Third Parties, even after consumers declined or rejected all cookies and tracking technologies by adjusting the available toggle switches on the cookies preferences window. All of these network calls are made to the Third Parties without the user’s knowledge, and despite the user’s rejection of all such cookies.

40. Plaintiffs' and other Website users' Private Communications, including their

1 browsing history, visit history, website interactions, user input data, demographic information,
2 interests and preferences, shopping behaviors, device information, referring URLs, session
3 information, user identifiers, and/or geolocation data, were surreptitiously obtained by the Third
4 Parties via these cookies.

5 41. As users interact with the Websites, even after adjusting the available toggle
6 switches on the Cookie Preference Center to the inactive position, thereby opting out of or
7 rejecting the use of cookies and similar technologies for personalized content, targeted
8 advertising, and providing third-party services, as well as the sale or sharing of the user's
9 personal information with third parties for such functions, or other purposes, more data regarding
10 users' behavior and communications are sent to third parties, alongside the cookie data. The
11 third-party cookies that Defendant wrongfully allows to be stored on users' devices and
12 browsers, and to be transmitted to the Third Parties, cause the Third Parties to track and collect
13 data on users' behaviors and communications, including Private Communications, on the
14 Websites. Because third-party cookies cause the Third Parties to track users' behavior across the
15 Internet and across time, user data can be correlated and combined with other data sets to compile
16 comprehensive user profiles that reflect consumers' behavior, preferences, and demographics
17 (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes).
18 These Third Parties monetize user profiles for advertising, sales, and marketing purposes to
19 generate revenue and target advertising to Internet users. Advertisers can gain deep
20 understanding of users' behavioral traits and characteristics and target those users with
21 advertisements tailored to their consumer profiles and audience segments.

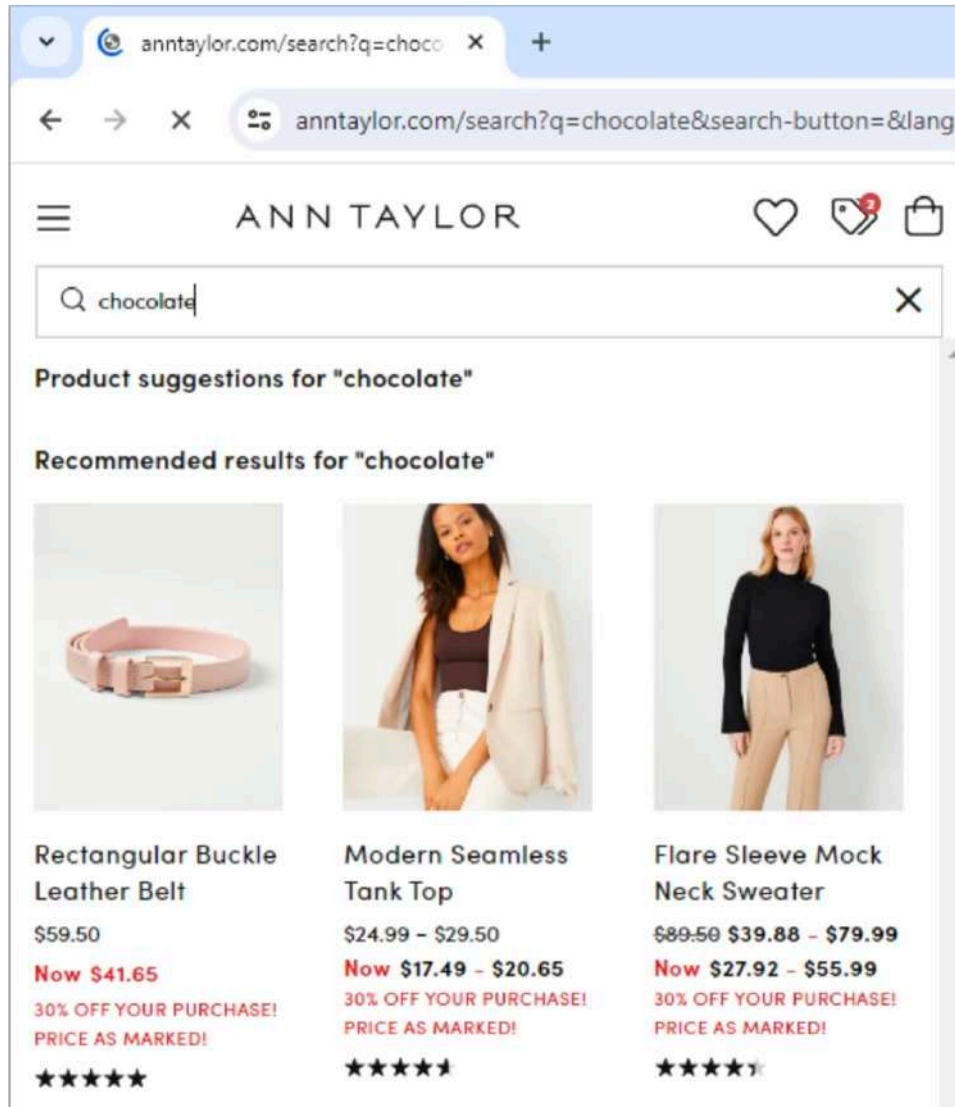
22 42. The Third Parties' code that the Websites cause to be loaded and executed by the
23 user's browser constitutes a wiretap because, when it is executed, it causes the Third Parties—
24 separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop
25 upon, record, extract data from, and analyze conversations to which they are not parties. When
26 the Third Parties use their respective wiretaps on the Websites users' Private Communications,
27 the wiretaps are not like tape recorders or "tools" used by one party to record the other. The
28 Third Parties each have the capability to use the contents of conversations they collect through

their respective wiretaps for their own purposes as described in more detail below.

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

1. The Websites Cause the Interception of the Contents of Communications.

43. The Websites include search bars and other input fields through which users enter information. For example, below is a screenshot of the search bar on the Ann Taylor website, where a user has entered the search term "chocolate":



44. The other Websites have search bars that look and operate substantially the same

² This section contains multiple examples of specific data being sent from a user's browser to third parties. Each example was collected after the user had rejected all non-strictly necessary cookies.

1 as the Ann Taylor search bar shown above.

2 45. When users input the information into these search fields, they intend to
3 communicate the contents of their searches directly to the Websites.

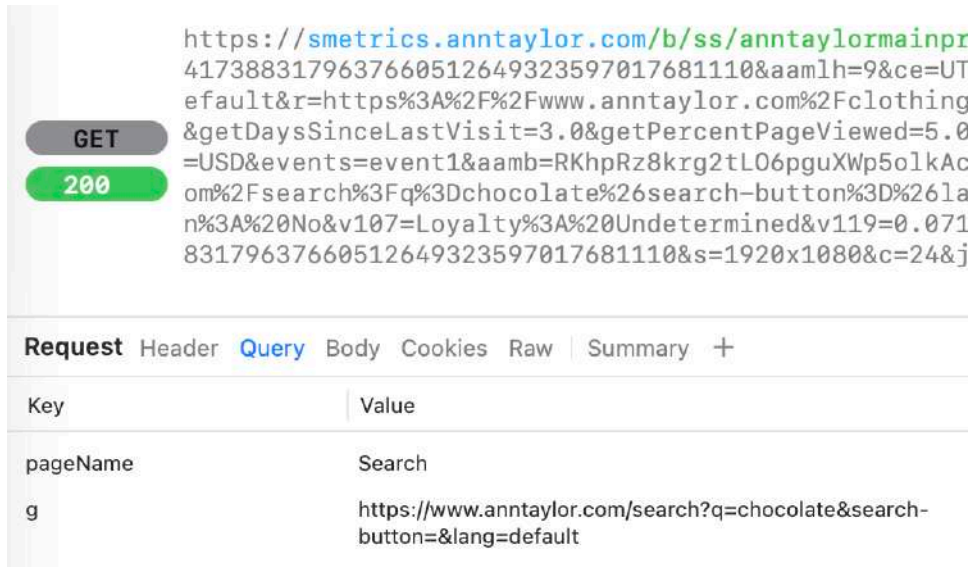
4 46. Instead, Defendant programmed the Websites such that the contents of those
5 communications are transmitted to, and intercepted by, the Third Parties while the
6 communications are in transit between users' browsers and the Websites.

7 47. For example, the Websites cause users' search queries to be transmitted along
8 with cookie data to third parties, including Google, even after users have rejected all unnecessary
9 cookies. When a user submits a search, the Website loads a results page that includes the user's
10 query in the URL. The Websites then transmit those URLs to third parties, thereby disclosing
11 the full search query to those parties. For instance, the test search string ("chocolate") depicted
12 above on the Ann Taylor Website was transmitted to Google's doubleclick.net domain, along
13 with associated identifiers and metadata:

GET	https://td.doubleclick.net/td/rul/1069304232?random
200	url=https%3A%2F%2Fwww.annaylor.com%2Fsearch%3Fq%3Dchocolate%3Fdwvar_832734_color%3D018845%26priceSort%3DDESC%3Fgtag.config
Request Header Query Body Cookies Raw Summary +	
Key	Value
async	1
auid	1973484373.1709137373
bg	ffffff
cv	11
data	event=gtag.config
dma	0
fledge	1
fmt	3
frm	0
fst	1709137515505
gcd	131313131
gtm	45be42q1v879552355za200
guid	ON
hn	www.googleadservices.com
npa	0
pscdl	noapi
random	1709137515505
ref	https://www.annaylor.com/clothing/jackets-and-blazers/cata000017/832734.html?dwvar_832734_color=018845&priceSort=DES
tiba	chocolate Ann Taylor
u_h	1080
u_w	1920
url	https://www.annaylor.com/search?q=chocolate&search-button=&lang=default

48. The user's communications are disclosed to Google in both the "tiba" and "url" parameters above.

49. Likewise, search terms are disclosed to Adobe via the web address smetrics.annaylor.com, which—despite appearances—is an alias for the domain annaylor.com.ssl.sc.omtrdc.net, which is owned and operated by Adobe.



50. The other Websites operate substantially the same, disclosing search terms and cookie data Google, Adobe, and other third parties without users' consent or knowledge.

2. Google Cookies.

51. Defendant causes third party cookies to be transmitted to and from the Websites users' browsers and devices, even after users reject all non-strictly necessary cookies (including advertising and analytics cookies) to and from the www.google.com, adservice.google.com, analytics.google.com, and doubleclick.net domains. Each of these domains is associated with Google LLC's digital advertising and analytics platform that collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.³ Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's DoubleClick cookies.⁴ Google's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. Further, by identifying users who have shown interest in certain products or content, Google's cookies cause its advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within

³ See Our advertising and measurement cookies (available at <https://business.safety.google/adscookies/>).

⁴ See, e.g. <https://www.ghostery.com/whotracksme/trackers/doubleclick>.

1 Google's ad network.⁵

2 52. Specifically, Google sends cookies when a web user visits a webpage that shows
3 Google Marketing Platform advertising products and/or Google Ad Manager ads.⁶ "Pages with
4 Google Marketing Platform advertising products or Google Ad Manager ads include ad tags that
5 instruct browsers to request ad content from [Google's] servers. When the server delivers the ad
6 content, it also sends a cookie. But a page doesn't have to show Google Marketing Platform
7 advertising products or Google Ad Manager ads for this to happen; it just needs to include
8 Google Marketing Platform advertising products or Google Ad Manager ad tags, which might
9 load a click tracker or impression pixel instead." *Id.* As Google explains, "Google Marketing
10 Platform advertising products and Google Ad Manager send a cookie to the browser after any
11 impression, click, or other activity that results in a call to our servers." *Id.*

12 53. Google also uses cookies in performing analytical functions. As Google explains,
13 "Google Analytics is a platform that collects data from [] websites and apps to create reports that
14 provide insights into [] business[es]."⁷ "To measure a website ... [one] add[s] a small piece of
15 JavaScript measurement code to each page on [a] site." *Id.* Then, "[e]very time a user visits a
16 webpage, the tracking code will collect ... information about how that user interacted with the
17 page." *Id.* Google Analytics enables website owners to "measure when someone loads a page,
18 clicks a link, [] makes a purchase;" "completes a purchase"; "searches [] website or app"; "select
19 content on [] website or app"; "views an item"; and "views their shopping cart."⁸

20 54. Google's cookies allow it to obtain and store at least the following user data:
21 (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data,
22 (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors,

23
24
25 ⁵ See, e.g. About cross-channel remarketing in Search Ads 360 (available at
<https://support.google.com/searchads/answer/7189623?hl=en>); About dynamic remarketing for retail (available at
<https://support.google.com/google-ads/answer/6099158?hl=en&sjid=1196213575075458908-NC>).

26 ⁶ 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>); see also Cookies
27 and user identification (available at <https://developers.google.com/tag-platform/security/concepts/cookies>).

28 ⁷ How Google Analytics Works (available at <https://support.google.com/analytics/answer/12159447?hl=en>).

⁸ Set up events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>); and
Recommended events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>).

(viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data—including whether a user is located in California.⁹

55. For example, the Google software code that Defendant causes to be stored on and executed by the Ann Taylor Website’s users’ devices causes the following data, including cookie data, to be sent to Google’s domain, at doubleclick.net after users have rejected non-strictly necessary cookies:

⁹ See About the Google Tag (available at <https://support.google.com/searchads/answer/7550511?hl=en>); How Floodlight Recognizes Users (available at <https://support.google.com/searchads/answer/2903014?hl=en>); How Google Ads tracks website conversions (available at <https://support.google.com/google-ads/answer/7521212>); Google Ads Help, Cookie: Definition (available at <https://support.google.com/google-ads/answer/2407785?hl=en>); About demographic targeting in Google Ads (available at https://support.google.com/searchads/answer/7298581?hl=en&sjid=1196213575075458908-NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1); How Google Analytics Works (available at <https://support.google.com/analytics/answer/12159447>); Set up events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>); and Recommended events (available at <https://support.google.com/analytics/answer/9267735>).

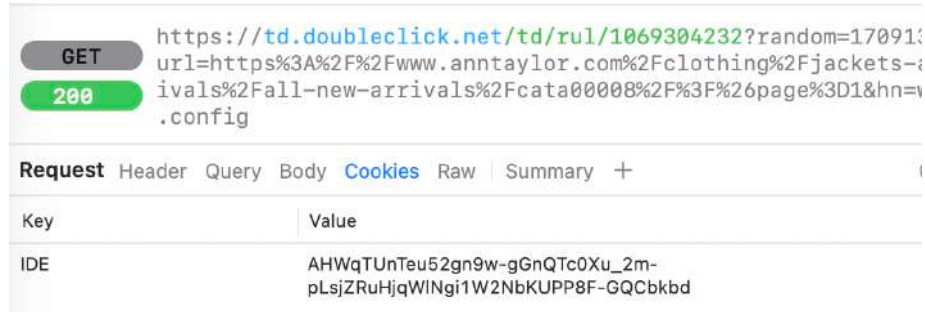
```
https://td.doubleclick.net/td/rul/1069304232?random=170911
url=https%3A%2F%2Fwww.annetaylor.com%2Fclothing%2Fjackets-&
ivals%2Fall-new-arrivals%2Fcata00008%2F%3F%26page%3D1&hn=v
.config
```

ivals%2Fall-new-arrivals%2Fcata00008%2F%3F%26page%3D1&hn=v
.config

 Springer

Key	Value
random	1709137503738
cv	11
fst	1709137503738
fmt	3
bg	ffffff
guid	ON
async	1
gtm	45be42q1v879552355za200
gcd	13I3I3I3I1
dma	0
u_w	1920
u_h	1080
url	https://www.anntaylor.com/clothing/jackets-and-blazers/cata000017/832734.html?dwvar_832734_color=018845&priceSort=DES
ref	https://www.anntaylor.com/new-arrivals/all-new-arrivals/cata00008/3&page=1
hn	www.googleadservices.com
frm	0
tiba	Tweed Cropped Jacket
npa	0
pscdl	noapi
auid	1973484373.1709137373
fledge	1
data	event=gtag.config

1	GET	https://td.doubleclick.net/td/rul/1069304232?random=1709137503738&cv=11&fst=1709137503738&fmt=3&bg=ffffff&guid=ON&async=1>m=45be42q1v879552355za200&gcd=131313131&dma=0&u_w=1920&u_h=1080&url=https%3A%2F%2Fwww.anntaylor.com%2Fclothing%2Fjackets-and-blazers%2Fcata000017%2F832734.html%3Fdwvar_832734_color%3D018845%26priceSort%3DDES&ref=https%3A%2F%2Fwww.anntaylor.com%2Fnew-arrivals%2Fall-new-arrivals%2Fcata00008%2F%3F%26page%3D1&hn=www.googleadservices.com&frm=0&tiba=Tweed%20Cropped%20Jacket&npa=0&pscdl=noapi&uid=1973484373.1709137373&fledge=1&data=event%3Dgtag.config
2	200	
3	Request	Header Query Body Cookies Raw Summary +
4	Key	Value
5	:authority	td.doubleclick.net
6	:method	GET
7	:path	/td/rul/1069304232? random=1709137503738&cv=11&fst=1709137503738&fmt=3&bg=ffffff&guid=ON&async=1>m=45be42q1v879552355za200&gcd=131313131&dma=0&u_w=1920&u_h=1080&url=https%3A%2F%2Fwww.anntaylor.com%2Fclothing%2Fjackets-and-blazers%2Fcata000017%2F832734.html%3Fdwvar_832734_color%3D018845%26priceSort%3DDES&ref=https%3A%2F%2Fwww.anntaylor.com%2Fnew-arrivals%2Fall-new-arrivals%2Fcata00008%2F%3F%26page%3D1&hn=www.googleadservices.com&frm=0&tiba=Tweed%20Cropped%20Jacket&npa=0&pscdl=noapi&uid=1973484373.1709137373&fledge=1&data=event%3Dgtag.config
8	:scheme	https
9	accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10	accept-encoding	gzip, deflate, br, zstd
11	accept-language	en-US,en;q=0.9
12	cookie	IDE=AHWqTUnTeu52gn9w-gGnQTc0Xu_2m-plSjZRuHjqWINGi1W2NbKUPP8F-GQCbkbd
13	priority	u=0, i
14	referer	https://www.anntaylor.com/
15	sec-ch-ua	"Chromium";v="122", "Not(A:Brand";v="24", "Google Chrome";v="122"
16	sec-ch-ua-mobile	?0
17	sec-ch-ua-platform	"Windows"
18	sec-fetch-dest	iframe
19	sec-fetch-mode	navigate
20	sec-fetch-site	cross-site
21	sec-fetch-user	?1
22	upgrade-insecure-requests	1
23	user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
24	x-client-data	CJC2yQEIpLbJAQipncoBCKL1ygEllaHLAQjwmM0BCIWgzQEIwe7NARjJ+M0BG0uNpRc=
25	Host	td.doubleclick.net



56. 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.

57. The “url” and “tiba” parameters disclose to Google the exact webpage and title that the user was viewing. Here, the user was viewing a page for a Tweed Cropped Jacket.

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

59. Google documentation confirms that the “IDE” cookie is used for advertising. Specifically, it is “used to show Google ads on non-Google sites.”¹⁰

60. Further, as shown above, the Google software code that Defendant causes to be stored on and executed by the user’s device causes the user’s “user-agent” information to be sent to Google.

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

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

63. The same is true of the Lane Bryant and Loft Websites—even after users reject cookies, Defendant causes tracking data and cookie data to be sent to Google.

64. Because Google’s cookies operate across multiple sites (i.e., cross-site tracking), the cookie causes Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google’s advertising platform

¹⁰ <https://policies.google.com/technologies/cookies?hl=en-US>.

1 aggregates user data to create consumer profiles containing detailed information about a
2 consumer's behavior, preferences, and demographics and audience segments based on shared
3 traits (such as females, Millennials, Californians, etc.), and to perform targeted advertising and
4 marketing analytics.

5 65. Thus, the Google cookies used on the Websites cause Google to track users'
6 interactions with advertisements to help advertisers understand how users engage with ads across
7 different websites. Further, the user data collected through the cookie enables the delivery of
8 personalized ads based on user interests and behaviors. For instance, if a user frequently visits
9 travel-related websites, Google will show her more travel-related advertisements. Further, the
10 collected data is used to generate reports for advertisers, helping them assess the performance of
11 their ad campaigns and make data-driven decisions (such as renaming their products). Further,
12 Google's advertising platform enables advertisers to retarget marketing, which Google explains
13 allows advertisers to "show previous visitors ads based on products or services they viewed on
14 your website. With messages tailored to your audience, dynamic remarketing helps you build
15 leads and sales by bringing previous visitors back to your website to complete what they
16 started."¹¹

17 66. Further, in its "Shared Data Under Measurement Controller-Controller Data
18 Protection Terms," Google states: "Google can access and analyze the Analytics data customers
19 share with us to better understand online behavior and trends, and improve our products and
20 services—for example, to improve Google search results, detect and remove invalid advertising
21 traffic in Google Ads, and test algorithms and build models that power services like Google
22 Analytics Intelligence that apply machine-learning to surface suggestions and insights for
23 customers based on their analytics data and like Google Ads that applies broad models to
24 improve ads personalization and relevance. These capabilities are critical to the value of the
25 products we deliver to customers today."¹² Thus, Google can have the capability to use the data
26

27 ¹¹ Dynamic remarketing for web setup guide (available at <https://support.google.com/google-ads/answer/6077124>).

28 ¹² Shared Data Under Measurement Controller-Controller Data Protection Terms (available at <https://support.google.com/analytics/answer/9024351>).

1 it collects for understanding online behavior and trends, machine learning, and improving its
2 own products and services.

3 **3. TikTok Cookies.**

4 67. Defendant also causes third party cookies to be transmitted to and from Website
5 users' browsers and devices, even after users elect to reject all non-strictly necessary cookies, to
6 and from the analytics.tiktok.com domain. This domain is associated with TikTok for Business,
7 a suite of tools offered by TikTok USDS Joint Venture LLC. The TikTok social media platform
8 is used to create and share short-form videos, and it utilizes cookies for various purposes
9 including assisting brands and marketers to create, manage, and optimize ad campaigns on the
10 platform.¹³

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

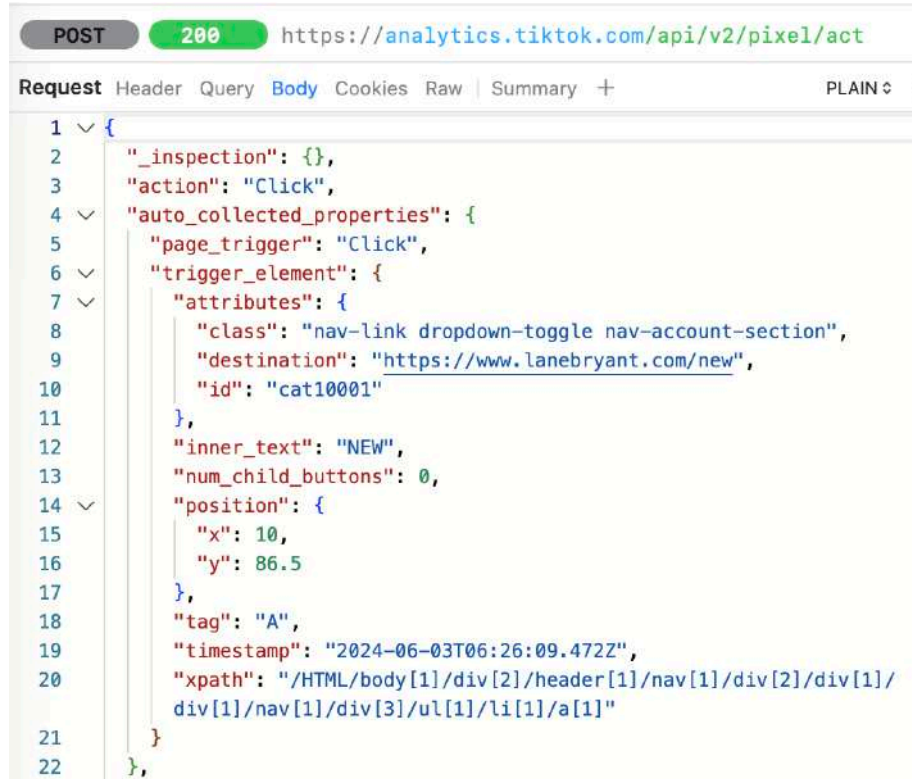
20 69. These cookies enable TikTok to obtain and store at least the following user data:
21 (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, including
22 *email addresses and phone numbers*; (v) demographic information, (vi) interests and
23
24
25

26 ¹³ See, e.g., TikTok for Business (<https://ads.tiktok.com/business/en-US/products/ads>; and
27 <https://ads.tiktok.com/business/en-US/products/measurement>); TikTok Business Help Center; Using Cookies with
28 TikTok Pixel (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

¹⁴ TikTok Business Help Center; Using Cookies with TikTok Pixel (available at
<https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

preferences, (vii) shopping behaviors, (viii) device information, (ix) session information, (x) user identifiers, and (xi) geolocation data in the form of the IP address.¹⁵

70. For example, the TikTok software code that Defendant causes to be stored on and executed by the Lane Bryant Website's users' devices causes the following data to be sent to TikTok's domain, at analytics.tiktok.com:



```

1  {
2    "_inspection": {},
3    "action": "Click",
4    "auto_collected_properties": {
5      "page_trigger": "Click",
6      "trigger_element": {
7        "attributes": {
8          "class": "nav-link dropdown-toggle nav-account-section",
9          "destination": "https://www.lanebryant.com/new",
10         "id": "cat10001"
11       },
12       "inner_text": "NEW",
13       "num_child_buttons": 0,
14       "position": {
15         "x": 10,
16         "y": 86.5
17       },
18       "tag": "A",
19       "timestamp": "2024-06-03T06:26:09.472Z",
20       "xpath": "/HTML/body[1]/div[2]/header[1]/nav[1]/div[2]/div[1]/div[1]/nav[1]/div[3]/ul[1]/li[1]/a[1]"
21     }
22   },

```

¹⁵ *Id.*; see also TikTok for Business: Enhance Data Postback with the TikTok Pixel (<https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel?lang=en>); TikTok for Business: Advanced Matching for Web (available at <https://ads.tiktok.com/help/article/advanced-matching-web?redirected=1>); TikTok for Business: About TikTok Pixel (available at <https://ads.tiktok.com/help/article/tiktok-pixel?lang=en>).

```

23  ✓ "context": {
24  ✓   "ad": {
25     "jsb_status": 2,
26     "sdk_env": "external"
27   },
28  ✓   "device": {
29     "platform": "pc"
30   },
31   "index": 0,
32  ✓   "library": {
33     "name": "pixel.js",
34     "version": "2.2.0"
35   },
36  ✓   "page": {
37     "load_progress": "2",
38     "referrer": "",
39     "url": "https://www.lanebryant.com/"
40   },
41   "pageview_id": "pageId-1717395912417-8789829161001.0.0",
42  ✓   "pixel": {
43     "code": "CAQTMHBC77U804GF3K70",
44     "codes": "CAQTMHBC77U804GF3K70",
45     "runtime": "1"
46   },
47   "session_id":
48   ✓   "user": {
49     "anonymous_id": "v6F11_KMFadJnok9JD1aA0MSm6P"
50   },
51   "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/
537.36",
52   "variation_id": "test_2_single_track"
53 },

54   "event_id": "",
55   "is_onsite": false,
56   "message_id": "messageId-1717395969472-8607211683012",
57   "properties": {},
58  ✓   "signal_diagnostic_labels": {
59  ✓     "hashed_email": {
60       "label": "missing"
61     },
62  ✓     "hashed_phone": {
63       "label": "missing"
64     },
65  ✓     "raw_auto_email": {
66       "label": "missing"
67     },
68  ✓     "raw_auto_phone": {
69       "label": "missing"
70     },
71  ✓     "raw_email": {
72       "label": "missing"
73     },
74  ✓     "raw_phone": {
75       "label": "missing"
76     }
77   },
78   "timestamp": "2024-06-03T06:26:09.472Z"
79 }

```

POST 200 https://analytics.tiktok.com/api/v2/pixel/act	
Request Header Query Body Cookies Raw Summary +	
Key	Value
:authority	analytics.tiktok.com
:method	POST
:path	/api/v2/pixel/act
:scheme	https
accept	*/*
accept-encoding	gzip, deflate, br, zstd
accept-language	en-US,en;q=0.9
content-length	1493
content-type	text/plain;charset=UTF-8
cookie	_ttp=2h1qdkveVwfYrFJsOWFfAcmwcR0
origin	https://www.lanebryant.com
priority	u=4, i
referer	https://www.lanebryant.com/
sec-ch-ua	"Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"macOS"
sec-fetch-dest	empty
sec-fetch-mode	no-cors
sec-fetch-site	cross-site
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host	analytics.tiktok.com

POST 200 https://analytics.tiktok.com/api/v2/pixel/act	
Request Header Query Body Cookies Raw Summary +	
Key	Value
_ttp	2h1qdkveVwfYrFJsOWFfAcmwcR0

71. 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.¹⁶

72. The data further discloses, among other things, the exact button that the user clicked on the Lane Bryant Website, the exact time—down to the millisecond—when it was clicked, and that the button led to the destination <https://www.lanebryant.com/new>.

¹⁶ See, e.g., How to get TikTok session id? (available at <https://gbtimes.com/how-to-get-tiktok-session-id/>).

73. As shown above, the TikTok software code that Defendant causes to be stored on and executed by the user's device also causes the "_ttp" cookie to be sent to TikTok.

74. 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."¹⁷

75. Further, as shown above, 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.

76. As discussed above with respect to Google, the "user-agent" corresponds to the device and browser that the user has used to access the Website.

77. 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.

78. By collecting this user data, TikTok performs user behavior tracking, i.e., monitoring user actions like page views, clicks, and interactions to understand user engagement; advertising optimization, i.e., gathering data to enhance the relevance and effectiveness of TikTok advertising campaigns; and performance measurement (i.e., assessing the success of marketing efforts by analyze user responses to ads and content).¹⁸

79. Further, TikTok's Automatic Advanced Matching feature functions as follows: "When a visitor lands on your website and inputs customer information during registration, sign-in, contact, or checkout on a website where you installed your pixel, Automatic Advanced Matching will capture information from those fields. ...TikTok will use hashed information to link event information to people on TikTok. TikTok may use matched events to better attribute events to TikTok ads, optimize advertisers' future campaigns, and depending on advertisers' and users' settings, TikTok may also add people to advertisers' retargeting or engagement audiences."¹⁹

¹⁷ See TikTok for Business: Using Cookies with TikTok Pixel (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

¹⁸ *Id.*

¹⁹ 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 **4. Adobe Cookies.**

2 80. Defendant also causes third party cookies to be transmitted to and from the
3 Websites' users' browsers and devices, even after users elect to opt out of or reject all cookies,
4 including all Advertising and Functional cookies, other than those strictly necessary for the
5 Websites to function, to and from various domains owned by Adobe Inc.

6 81. For example, Defendant has configured a subdomain it owns and operates, at
7 smetrics.anntaylor.com, to point directly to Adobe's endpoint, at
8 anntaylor.com.ssl.sc.omtrdc.net:²⁰

9

10

11

12

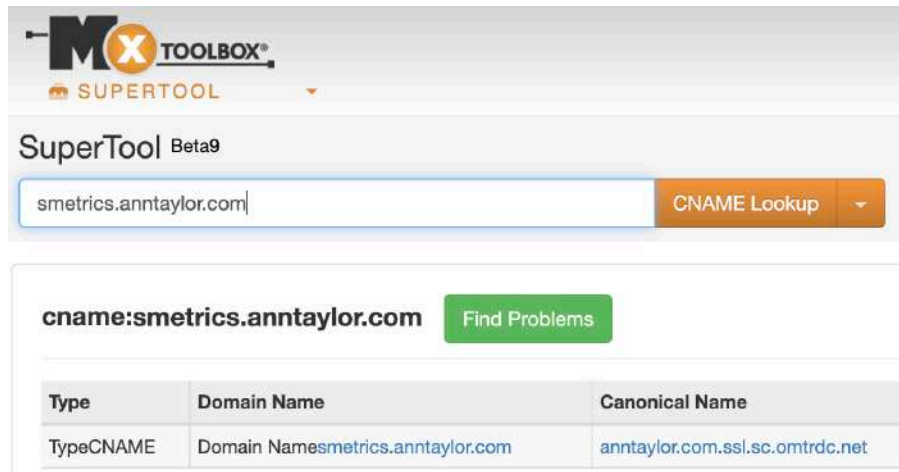
13

14

15

16

17



The screenshot shows the MX Toolbox SuperTool interface. At the top, there is a logo for 'MX TOOLBOX' and 'SUPERTOOL'. Below the logo, the text 'SuperTool Beta9' is displayed. A search bar contains the domain 'smetrics.anntaylor.com', and a button labeled 'CNAME Lookup' is next to it. Below the search bar, the text 'cname:smetrics.anntaylor.com' is shown, followed by a green button labeled 'Find Problems'. Below this, a table displays the lookup results.

Type	Domain Name	Canonical Name
TypeCNAME	Domain Namesmetrics.anntaylor.com	anntaylor.com.ssl.sc.omtrdc.net

18 82. The omtrdc.net domain is owned and operated by Adobe, and functions as a
19 tracking server for Adobe Analytics.²¹

20 83. The same is true of the other Websites:

21

22

23

24

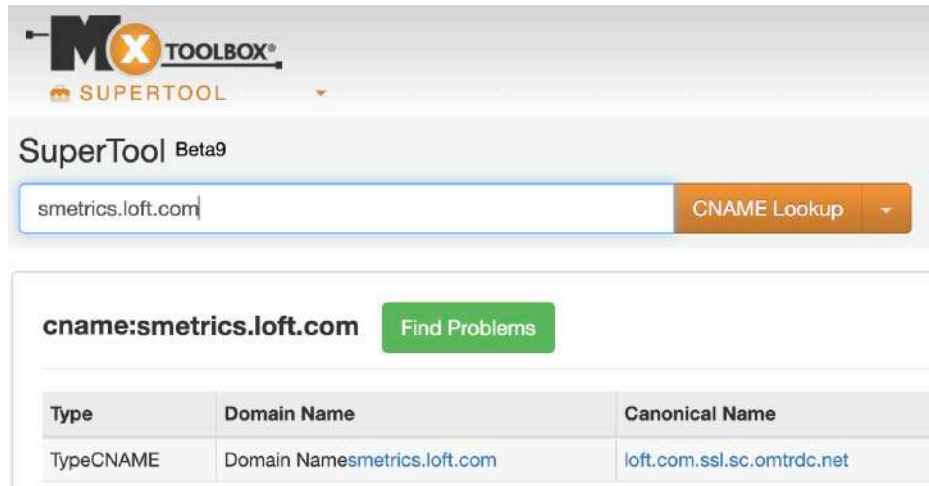
25

26

27 ²⁰ Data obtained from <https://mxtoolbox.com>.

28 ²¹ See <https://experienceleague.adobe.com/en/docs/target/using/integrate/a4t/analytics-tracking-server>.

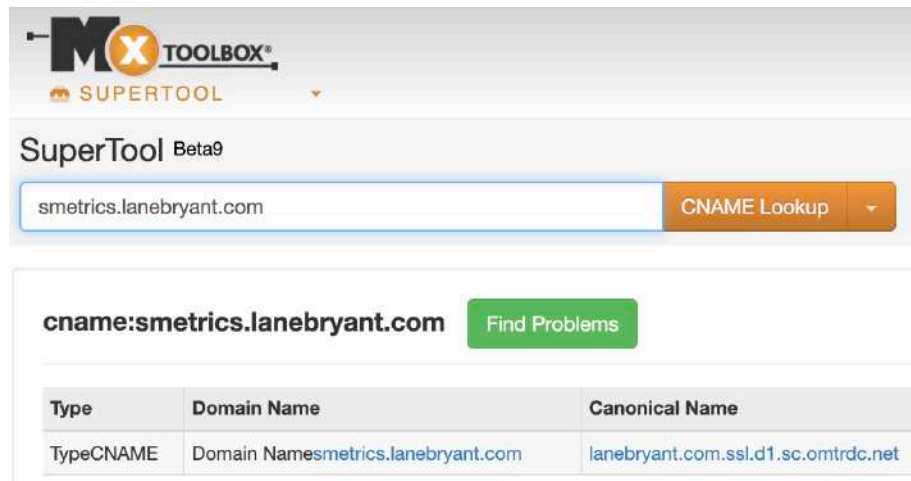
1
2
3
4
5
6
7
8
9



The screenshot shows the MX Toolbox SuperTool Beta9 interface. At the top, there is a search bar containing the text "smetrics.loft.com" and a "CNAME Lookup" button. Below the search bar, the text "cname:smetrics.loft.com" is displayed next to a green "Find Problems" button. A table below shows the results of the lookup.

Type	Domain Name	Canonical Name
TypeCNAME	Domain Namesmetrics.loft.com	loft.com.ssl.sc.omtrdc.net

10
11
12
13
14
15
16
17
18



The screenshot shows the MX Toolbox SuperTool Beta9 interface. At the top, there is a search bar containing the text "smetrics.lanebryant.com" and a "CNAME Lookup" button. Below the search bar, the text "cname:smetrics.lanebryant.com" is displayed next to a green "Find Problems" button. A table below shows the results of the lookup.

Type	Domain Name	Canonical Name
TypeCNAME	Domain Namesmetrics.lanebryant.com	lanebryant.com.ssl.d1.sc.omtrdc.net

19 84. When a user visits any of the Websites, the Website code causes multiple network
20 calls to be made to Adobe throughout the user's visit. For instance, when a user searches for the
21 term "chocolate" on the any of the Websites, the Website causes the following type of data—
22 including cookie data—to be sent to Adobe:
23
24
25
26
27
28

GET

200

https://smetrics.anntaylor.com/b/ss/anntaylormainpro4173883179637660512649323597017681110&aamlh=9&ce=UTFchocolate%26search-button%3D%26lang%3Ddefault&c.&get.1&getQueryParam=4.0.1&pt=3.0&getValOnce=3.0.1&getPaXW5X3_3mrnaNgC5f10L5JMjkmV3050%3D&c17=https%3A%2F%2FN&v106=Login%3A%20No&v107=Loyalty%3A%20Undetermined&&a.&activitymap.&page=Search&link=Ascena®ion=hdc-

Request

Header

Query

Body

Cookies

Raw

Summary

+

Key	Value
.a	
.activitymap	
.c	
.c	
.cm	
a.	
aamb	RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y
aamlh	9
activitymap.	
apl	4.0
AQB	1
AQE	1
bh	953
bw	527
c	24
c.	
c.	

c17	https://www.anntaylor.com/
c3	home
c67	Login: No
c68	Loyalty: Undetermined
cc	USD
cdp	2
ce	UTF-8
cm.	
events	event240=7.68
fpCookieDomainPeriods	2
g	https://www.anntaylor.com/
getDaysSinceLastVisit	3.0
getNewRepeat	3.0.1
getPageLoadTime	3.1
getPercentPageViewed	5.0.2
getPreviousValue	3.0.1
getQueryParam	4.0.1
getValOnce	3.0.1
handlePPVevents	4.0
inList	3.0
j	1.6
k	Y
link	Ascena

mcorgid	B6761CFE533096CB0A490D45@AdobeOrg
mid	84173883179637660512649323597017681110
ndh	1
p_fo	3.0
page	Search
pageIDType	1
pageName	Homepage
pf	1
pt	3.0
r	https://www.anntaylor.com/search?q=chocolate&search-button=&lang=default
region	hdc-wrapper
s	1920x1080
sdid	0723EF9B9461A24F-18D26D78D46B609D
ssf	1
t	28/1/2024 11:25:25 3 300
v	N
v106	Login: No
v107	Loyalty: Undetermined
v119	0.07140408770105489_1709137370787
v122	https://www.anntaylor.com/
v123	84173883179637660512649323597017681110
v125	Search
v14	RnXuyXW5X3_3mrnaNgC5fIOL5JMjkmV3O50=
v18	New
v19	Weekday
v20	Wednesday
v27	ANN TAYLOR
v45	Homepage
v70	N

1 <https://smetrics.anntaylor.com/b/ss/anntaylormainpro>
2 [4173883179637660512649323597017681110&aamlh=9&ce=UTF](https://smetrics.anntaylor.com/b/ss/anntaylormainpro)
3 [chocolate%26search-button%3D%26lang%3Ddefault&c.&get](https://smetrics.anntaylor.com/b/ss/anntaylormainpro)
4 [.1&getQueryParam=4.0.1&pt=3.0&getValOnce=3.0.1&getPa](https://smetrics.anntaylor.com/b/ss/anntaylormainpro)
5 [XW5X3_3mrnaNgC5f10L5JMjkmV3050%3D&c17=https%3A%2F%2F](https://smetrics.anntaylor.com/b/ss/anntaylormainpro)
6 [N&v106=Login%3A%20No&v107=Loyalty%3A%20Undetermined&](https://smetrics.anntaylor.com/b/ss/anntaylormainpro)
7 [&a.&activitymap.&page=Search&link=Ascena®ion=hdc-](https://smetrics.anntaylor.com/b/ss/anntaylormainpro)

8 **GET**

9 **200**

Request	Header	Query	Body	Cookies	Raw	Summary	+
Key	Value						
priority	i						
referer	https://www.anntaylor.com/						
sec-ch-ua	"Chromium";v="122", "Not(A:Brand";v="24", "Google Chrome";v="122"						
sec-ch-ua-mobile	?0						
sec-ch-ua-platform	"Windows"						
sec-fetch-dest	image						
sec-fetch-mode	no-cors						
sec-fetch-site	same-site						
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36						
Host	smetrics.anntaylor.com						

https://smetrics.anntaylor.com/b/ss/anntaylormainpro
 4173883179637660512649323597017681110&aam1h=9&ce=UTF
 chocolate%26search-button%3D%26lang%3Ddefault&c.&get
 .1&getQueryParam=4.0.1&pt=3.0&getValOnce=3.0.1&getPa
 XW5X3_3mrnaNgC5f10L5JMjkmV3050%3D&c17=https%3A%2F%2F
 N&v106=Login%3A%20No&v107=Loyalty%3A%20Undetermined&
 &a.&activitymap.&page=Search&link=Ascena®ion=hdc-

GET

200

Request Header Query Body Cookies Raw Summary +

Key	Value
__cq_seg	0~0.00!1~0.00!2~0.00!3~0.00!4~0.00!5~0.00!6~0.00! 7~0.00!8~0.00!9~0.00
__cq_uuid	acBqc1xa2Cfa0IKoIFMXIeQLss
__ogfpid	1a74c978-544d-449d-8bbb-8c241f8553bf
__pxvid	9ded7506-d655-11ee-a83f-0242ac120003
__rcmp	0! bj1fZ2MsZj1nYyxzPTEsYz0xNDMwLHRyPTEwMCxybj04Njls dHM9MjAyNDAYMjguMTYyMixkPXBjO249c2lxLGy9c2lscz0x LGM9MTAwMyx0PTIwMTYwODE2LjAwMDk7bj1ydyxmPXJ3L HM9MSxjPTEwMDAsdD0yMDE2MDgxNi4wMDA3
__rpck	0! PTAhZXIKME55STZIMzBzSW5RM2RpSTZIMzBzSW1Waklqb 3hMQ0owT0NJNmV5SXhJam94TnpBNU1UTTNNek01TIRZe GZYMh4~
__rpckx	0! eyJ0Nyl6eyl1ljoXNzA5MTM3NTI0NjY1fSwidDd2ljp7ljUiOjE3 MDkxMzc1MjQ2NjV9LCJlYyI6Mn0~
__ruid	166591726-8u-l4-4k-1p- r2zte9cmp69ja4zx1chz-1709137371358

__rutma	166591726-8u-l4-4k-1p-r2zte9cmp69ja4zx1chz-1709137371358.1709137371358.1709137371358.1.5.5
__rutmb	166591726
_cs_c	0
_cs_cvars	%7B%221%22%3A%5B%22Page%20Name%22%2C%22Search%22%5D%2C%22%22%3A%5B%22Page%20Type%22%2C%22search%22%5D%2C%225%22%3A%5B%22Department%20Name%22%2C%22SEARCH%20RESULTS%22%5D%2C%229%22%3A%5B%22Product%20Category%20ID%22%2C%22cata00008%22%5D%2C%2210%22%3A%5B%22Product%20Cat%20Name%22%2C%22All%20New%20Arrivals%22%5D%2C%2211%22%3A%5B%22Cart%20Items%20Count%22%2C%220%22%5D%7D
_cs_id	2ee11dd8-2aff-ad40-8a4a-309f165fcbdc.1709137374.1.1709137516.1709137374.1.1743301374809.1
_cs_mk_aa	0.07140408770105489_1709137370787
_cs_s	3.5.0.1709139316311
_fbp	fb.1.1709137375488.1012316112
_ga	GA1.2.1982569732.1709137375
_ga_KLH5L175DT	GS1.1.1709137375.1.1.1709137516.60.0.0
_gat_gtag_UA_1742309_2	1
_gcl_au	1.1.1973484373.1709137373
_gid	GA1.2.902653848.1709137375
_pin_unauth	dWikPU1qZGlaR05sWmpFdE9HSmpOeTAwTWpNMkxUazFZak10WIRFNVI6VTFPRE5sTm1aaQ

_px3	6ffecc863b23598a83424885df81faafae223fa7870d3e913 4681150d174404d:hF3BeUoQnLlp1x2TBVOZ/ tuHGVmtwZWvwaabe4pwaizJgSHdsjdPqLuwKP2Aq3+VBQw pJ0cCOI7kH1MEOxxWRw==:1000:YV+kccjUmAqJF3jSvYH/ kXd6ff+9Nxx5PDp9c7ReXQPIGgrl/lhcG+FWj1Pxc+/ QfP4vKy9Ylp0PhUfbBXp56JQmD04c// 3y5Bfi4c4q8fNYDhIWVa2nIJdZzMthEpwK1OUS3WcUCTIn s9F6p2R+mJx3p7FFqsfWsGemh+swZXOkMMrl8vVdlPGUXv TNfANY1xHOTAmDa8OvUv1rMofQThKebJPHHD/ YbFSAKYzA/w=
_pxvid	895362fa-d655-11ee-bf95-8b865e2a5df0
_svsid	92c7e26ca46add5987616876eb783ddd
_svsidss	92c7e26ca46add5987616876eb783ddd
_tt_enable_cookie	1
_ttp	EykqK7qbe6SbK24xJODEgyeYBu-
_uetsid	a084dc40d65511ee9a5c83e55550495a
_uetvid	a0852a60d65511ee9d64936e646e5c64
AMCV_B6761CFE533096CB0 A490D45%40AdobeOrg	179643557%7CMCMID%7C84173883179637660512649 323597017681110%7CMCAAMLH-1709742294%7C9%7 CMCAAMB-1709742294%7CRKhpRz8krg2tLO6pguXWp5ol kAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-170 9144694s%7CNONE%7CMCAID%7CNONE%7CvVersion%7 C5.5.0%7CMCIDTS%7C19782
AMCVS_B6761CFE533096CB 0A490D45%40AdobeOrg	1
at_check	true
bfx.apiKey	fb884980-4659-11ed-a528-2d79ad770444
bfx.country	US
bfx.currency	USD

bfX.env	PROD
bfX.isInternational	false
bfX.language	en
bfX.logLevel	ERROR
bfX.sessionId	28c49615-55b5-4a5f-a1cd-09b554c72b1d
cr18.fpcuid	d16ad394-89f4-4f55-9f83-5e1ada56dec4
cto_bundle	zq3Ub184MUQ3YmJ1NFdhNmY1T20xSEdmdnY2MFMxZ1c 2cTE1QWFhOVpPOFPqb2dmMDFmaTBydUdvd1FDWVhjJTJ CRnN0enZNYUJsZE1OZHnkNSUyQjkxeFolMkZwamtic0Y1J TJCYIJoyTFXZEtxb1o1JTJCNEJXcnolMkYIMkZlcUNEbzBYW GUIIMkYIMkZsTnh1biUyQjhyNTRoYnZkV3cxUkgwbkhnYXklM kJTdGIWelAxa2xPWxIZMHBNT3M5QUZJVVNFJTNE
dtm_token	AQEDV0ywgisoOAEm0W6hAQElagE
dtm_token_sc	AQEDV0ywgisoOAEm0W6hAQEBAQA
forterToken	559d6d7ed52f49318a37bb58abf50078_1709137524747_ _UDF43-m4_15ck
mbox	session#7a8e68face184549b790391ed786420f#1709139 384 PC#7a8e68face184549b790391ed786420f.35_0#177238 2324
mp_ann_taylor_mixpanel	%7B%22distinct_id%22%3A%20%2218df086ab70812-05 a0f9c489c52d-26001b51-1fa400-18df086ab7110d3%22 %2C%22bc_persist_updated%22%3A%20170913737407 2%7D
OptanonAlertBoxClosed	2024-02-28T16:24:12.768Z
OptanonConsent	consentId=839071e8-b18b-4506-8c3f- c03f9e43fc21&datestamp=Wed+Feb+28+2024+11%3A25 %3A21+GMT-0500+ (Eastern+Standard+Time)&version=6.39.0&interactionCount =1&isGpcEnabled=0&isIABGlobal=false&hosts=&landingPat h=NotLandingPage&groups=BG80%3A0%2CC0004%3A0% 2CC0005%3A0%2CC0003%3A0%2CC0001%3A1%2CC00 02%3A1&geolocation=US%3BTX&AwaitingReconsent=false
pxcts	9daf5c8b-d655-11ee-944c-1c4394d612ef
QuantumMetricSessionID	1c4d6f5eff18980fc459eed5be97b401
QuantumMetricUserID	c971f027edc0dbcdde99878e596e193a
s_cc	true
s_dslv	1709137524035
s_ecid	MCMID%7C841738831796376605126493235970176811 10
s_nr30	1709137524873-New
s_sq	%5B%5BB%5D%5D

1 85. The “mid” parameter is Adobe’s unique user identifier that persists across
2 sessions, used to identify a visitor in the Adobe ecosystem.²²

3 86. The “r” parameter discloses the user’s search term (i.e., “chocolate”) to Adobe,
4 and further discloses that the user clicked the search button.

5 87. The “pageName” parameter tells Adobe what page the user is browsing on the
6 Website.

7 88. The “s” parameter tells Adobe the user’s screen resolution.

8 89. According to Adobe documentation, the cookies beginning with “AMCV_...” and
9 “AMCVS_...” are tracking cookies, enabling Adobe to identify the unique user and to track them
10 across other Adobe-integrated websites.²³

11 90. The “s_cc” cookie, set to “true” as it is here, tells Adobe that cookies are enabled.

12 91. In addition, the majority of the cookies above pertain to other third parties. For
13 example, the cookies beginning with “_ga” and “GA” are cookies set by Google Analytics. The
14 “QuantumMetric...” cookies pertain to Quantum Metric, a third-party tracking site. The cookies
15 beginning with “_tt...” are TikTok cookies. These cookies should not be sent to Adobe at all,
16 and are sent only because Defendant misconfigured its Websites. Nevertheless, these cookies
17 enable Adobe to further identify and track users with the specific identifiers contained within the
18 cookies.

19 92. Further, as shown above, the Adobe software code that Defendant causes to be
20 stored on and executed by the user’s device causes the user’s “user-agent” information to be sent
21 to Adobe. Each causes tracking data and cookie data to be sent to Adobe even after the user has
22 rejected cookies.

23 93. Finally, the data sent to Adobe includes the user’s IP address.

24 94. Each of the Websites is configured substantially the same with respect to the type
25 of data that is sent to the Adobe websites.

27 ²² See <https://experienceleague.adobe.com/en/docs/analytics/components/metrics/unique-visitors>

28 ²³ See <https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies>

95. In addition, at least the Loft and Ann Taylor Websites cause data—including cookie data—to be sent to dpm.demdex.com, which is associated with Adobe Inc.’s Audience Manager, a data management platform, Adobe’s Marketing Cloud, and Adobe’s Experience Cloud Identity Service, a service which provides a universal, persistent ID to identify visitors across all Adobe products.

96. The cookies sent to Adobe cookies are used to assign a unique identifier to each site visitor, which enables Adobe to consistently recognize and track users across different sessions and domains (i.e., cross-site tracking) and collect and synchronize user data to comprehensively observe and evaluate user behavior online.²⁴ These cookies enable Adobe to obtain and store at least the following user data: (i) user identifier; (ii) website interactions; (iii) browsing history; (iv) visit history; (v) interests and preferences; and (vi) session information.²⁵

97. Adobe aggregates this cookie data with other data from multiple channels and devices, including web analytics, CRM systems, and e-commerce platforms, to create consumer profiles containing detailed information about a consumer’s behavior, preferences, and demographics, create audience segments based on shared traits (such as millennials, tech enthusiasts, etc.), and to enable targeted advertising and marketing analytics.²⁶

5. Additional Third-Party Cookies

98. Defendant also causes third party cookies to be transmitted to and from Website users’ browsers and devices, even after users elect to “Reject All” cookies, to and from other domains, including p.cquotient.com, snapchat.com, everesttech.net, pinterest.com, mountain.com, openx.net, and insight.adsrvr.org.

²⁴ See, e.g., Adobe Experience League: Adobe Analytics cookies (available at <https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/analytics>); see also Adobe Experience League: Audience Manager cookies (available at <https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager>).

²⁵ See, e.g., Adobe Audience Manager User Guide: Data Collection Components (available at <https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/system-components/components-data-collection>).

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

99. The p.cquotient.com domain is associated with Salesforce, the company that owns and is responsible for CQuotient, is a multi-billion-dollar software company that provides software applications focused on sales, customer service, marketing automation, e-commerce, and analytics.²⁷ CQuotient is a “customer prediction platform” provided as an “analytic software that enables multi-channel retailers to understand their customers.”²⁸ Originally a separate company, CQuotient has since been acquired by Salesforce and folded into its Commerce Cloud or Unified Commerce suite of software applications.²⁹ These applications now feature “powerful AI that proactively helps merchants with storefront setup and channel optimization[.]”³⁰ While the Commerce Cloud includes tools for e-commerce that allow users to purchase products from websites, it also includes an analytic component that observes user interactions with a website in real time to make “personalized offers” to users based on their behavior.³¹ All of this occurs without user knowledge or consent and, on information and belief, it occurs on Defendant’s Websites where the CQuotient cookie is present, even after users opt out of or reject all such cookies, including all Advertising and Functional cookies.

100. The domain snapchat.com is associated with Snap Inc., the social media company that owns Snapchat. Snapchat is multimedia messaging app that lets users share photos, videos, text, and drawings—often designed to disappear after being viewed. Snapchat uses cookies to collect identifying data and data on users’ browsing history, choices, and interactions with advertisements.³² This data helps Snap personalize ad content and track users across the internet.³³ As Snap explains, it uses the data collected by Snapchat cookies “for optimization,

²⁷ <https://en.wikipedia.org/wiki/Salesforce>

²⁸ <https://pitchbook.com/profiles/company/51447-34#overview>

²⁹ *Id.*

³⁰ <https://www.salesforce.com/commerce/?cc=dwdcmain>

³¹ <https://www.salesforce.com/commerce/innovations/>

³² See, e.g., <https://businesshelp.snapchat.com/s/article/snap-privacy-faq>; <https://businesshelp.snapchat.com/s/article/snap-pixel-about>; <https://businesshelp.snapchat.com/s/article/conversions-api>; and <https://marketingapi.snapchat.com/docs/conversion.html?shell#conversion-parameters>.

³³ *Id.*

1 custom audience creation, look-alike modeling, reporting, machine learning, and targeting
2 capabilities. All uses are ... meant to deliver better results for our ad products.”³⁴

3 101. The **everesttech.net** subdomain is associated with Everest Technologies, Inc., a
4 technology company that provides data analytics and digital services.³⁵ The cm.everesttech.net
5 domain collects and transmits user data (including, “IP address, device information, browser
6 type and settings and information about your activity on the website . . . [and] pages and files
7 viewed, searches and other actions you take such as what features you use [on the website].”³⁶
8 Although Everest represents that such data may be used for operational purposes, it is also used
9 for advertising, analytics, and related data-driven services.

10 102. The **pinterest.com** domain is associated with Pinterest, Inc., a popular social
11 media platform that allows users to discover, save, and share ideas as pins in the form of photos
12 and videos. Businesses can upload and showcase their products through “Shop the Look” pins
13 or Product Pins that directly link to e-commerce websites. Businesses install the Pinterest tag on
14 their websites to track ad conversions. As Pinterest explains, “The Pinterest tag is a piece of code
15 that you add to your website. It lets Pinterest track visitors to your site, as well as the actions
16 they take on your site after seeing your Pinterest ad. This means you can measure how effective
17 your Pinterest ads are by understanding the actions people take on your website after seeing or
18 engaging with your ad.”³⁷ Pinterest cookies can be used to identify and track people who
19 purchase products, add items to a shopping cart, visit specific pages on the website, and/or search
20 for specific items on the website.³⁸

21
22
23 ³⁴ Snap Business Help Center, Pixel Implementation FAQs (available at
24 <https://businesshelp.snapchat.com/s/article/snap-pixel-faq>).

25 ³⁵ <https://www.everesttech.com/services/?c=us>.

26 ³⁶ *Id.*

27 ³⁷ Pinterest Help Center: Install the Pinterest Tag (available at <https://help.pinterest.com/en/business/article/install-the-pinterest-tag>).

28 ³⁸ *See, e.g.*, Pinterest Help Center: Add event codes (available at <https://help.pinterest.com/en/business/article/add-event-codes>); Pinterest Help Center: View tag parameters and cookies (available at <https://help.pinterest.com/en/business/article/pinterest-tag-parameters-and-cookies>).

103. The mountain.com domain is associated with MNTN, Inc., a company that builds advertising software for brands to generate targeted advertising, revenue, and site visits. MNTN uses these cookies to collect information about users' online activity, including behavioral data and website activity. As MNTN acknowledges, this information may directly or indirectly identify individual users. MNTN cookies are also used for advertising and targeted tracking of users. MNTN also offers a "Reporting Suite" to its customers that allows customers who use the mountain.com cookie on their websites to view order IDs and timestamps as well as individual keywords inputted into those websites by users.

104. The openx.net domain is associated with OpenX Technologies, Inc., a digital advertising technology company that operates a programmatic ad exchange.³⁹ OpenX uses cookies to facilitate the buying and selling of digital advertising. These cookies assign unique online identifiers to users, which are used to collect data across different websites about their online activity, browsing history, and inferred interests.⁴⁰ This information enables interest-based advertising, allowing advertisers to target specific users with relevant ads. The platform also uses cookies for ad delivery management, such as controlling ad frequency, measuring campaign performance, and syncing user identifiers with other advertising partners.⁴¹

105. The insight.adsrvr.org domain is associated with The Trade Desk, Inc., a digital advertising company that offers a cloud-based ad-buying platform that enables businesses to plan, manage, optimize, and measure data-driven digital advertising campaigns.⁴² The Trade Desk uses insight.adsrvr.org cookies to collect data on users such as their geographic locations, the type of device users are using, and users' interests as inferred from their web browsing or app usage activity.⁴³ This data helps The Trade Desk personalize ad content and track users across the internet.⁴⁴

³⁹ See <https://www.openx.com/publishers/ad-exchange/>.

⁴⁰ See <https://www.openx.com/privacy-center/ad-exchange-privacy-policy/>.

⁴¹ See *id.*

⁴² See The Trade Desk, Inc. 2023 Form 10-K (filed February, 15 2024).

⁴³ *Id.*

⁴⁴ *Id.*

106. The Trade Desk acknowledges that its cookies’ ability “to collect, augment, analyze, use and share data relies upon the ability to uniquely identify devices across websites and applications, and to collect data about user interactions with those devices for purposes such as serving relevant ads and measuring the effectiveness of ads.”⁴⁵

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

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

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

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

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

⁴⁵ *Id.*

1 reliability.⁴⁶ Third Party platforms encourage this redundant configuration and automatically
 2 compare identifiers contained within the transmitted data—such as event identifiers and device
 3 identifiers—to determine whether multiple transmissions correspond to the same user action.
 4 This deduplication occurs as the communications are received, before they are stored.

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

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

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

23 114. On information and belief, the Third Parties use ingest-phase processing
 24 platforms that perform real-time analytics and filtering on incoming data streams before storage.
 25 For example, Google developed MillWheel, an internal stream processing system, as well as
 26

27 ⁴⁶ For example, Google’s server-to-server API is the **Google Ads Conversion API**. TikTok uses the **TikTok Events**
 28 **API**. Snapchat’s is the **Snapchat Conversions API**. Pinterest’s uses the **Pinterest Conversions API**. On
 information and belief, each of the Third Parties uses a server-to-server API to collect user data.

Flume/FlumeJava, which evolved into Google Cloud Dataflow.⁴⁷ Google Cloud Dataflow enables Google to perform many functions on real-time data at the “Ingest” phase, before it is stored.⁴⁸ Google, which sells Dataflow to third party developers for use with their own products, states that Dataflow is used “to create data pipelines that read from one or more sources, ***transform the data***, and write the data to a destination.”⁴⁹ One use for Dataflow is the “[r]eal-time machine learning (ML) analysis of streaming data.”⁵⁰ Google confirms that Dataflow is “suitable for more advanced applications, such as real-time streaming analytics.”⁵¹

115. Pinterest uses Apache Kafka, a third-party real-time stream processing platform.⁵² The Kafka system streams events in real time to “many applications, such as native Kafka clients, Kafka Streams, Flink, and Spark streaming, which are consumers of a subset of Kafka topics that build several real-time pipelines.”⁵³ These systems “include but are not limited to monetization, safety and spam detection, metrics processing, and experimentation use cases.”⁵⁴

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

⁴⁷ See, e.g., Google Cloud Blog, “How cloud batch and stream data processing works” (August 2020), <https://cloud.google.com/blog/products/data-analytics/how-cloud-batch-and-stream-data-processing-works>.

⁴⁸ Google Cloud Blog, “BigQuery explained: An overview of BigQuery’s architecture” (September 2, 2020), <https://cloud.google.com/blog/products/data-analytics/new-blog-series-bigquery-explained-overview>.

⁴⁹ Google Cloud Documentation, “Dataflow overview,” <https://docs.cloud.google.com/dataflow/docs/overview> (emphasis added).

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² Confluent, “Lessons Learned from Running Apache Kafka at Scale at Pinterest,” <https://www.confluent.io/blog/running-kafka-at-scale-at-pinterest/>.

⁵³ *Id.*

⁵⁴ *Id.*

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

117. The “signaling” and “addressing” information captured and recorded by the Third Parties includes TCP and/or UDP port numbers associated with outgoing communications initiated by Plaintiffs’ and Class Members’ browsers and devices. In the context of Internet Protocol (IP) networking, port numbers function as sub-addresses that direct traffic to specific software processes. By recording these port numbers, the Third Parties identify and distinguish specific network connections and the communicating endpoints involved (e.g., a Plaintiff’s or Class Member’s IP address and TCP/UDP source port communicating with a Third Party’s destination IP address and destination port such as 443). These port numbers constitute addressing information associated with the communications initiated by Plaintiffs’ and Class Members’ browsers and devices and fall within the “instruments” and “facilities” contemplated by California Penal Code § 638.50(b).

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

119. Additionally, the Third Parties record HTTP request header metadata, such as the “Host” header and connection-management headers (e.g., “Connection” in HTTP/1.1), which function as digital “dialing” information. Just as a traditional pen register records the number dialed to reach a destination, these headers identify the intended web origin (via “Host”) and specify how the client requests the connection be handled for that request (e.g., whether to keep the connection open). This header information is transmitted as part of the Plaintiffs’ and Website users’ HTTP requests and, together with the destination network address and port,

1 enables the receiving Third Party to identify and log the destination and handling characteristics
2 of Plaintiffs' and Website users' communications, separate from any underlying user input or
3 message content.

4 120. Finally, the Third Parties' receiving infrastructure (e.g., servers, edge services,
5 and/or load balancers) observes and records network-level and transport-level routing and
6 addressing metadata associated with communications initiated by Plaintiffs' and Website users'
7 browsers and devices. This metadata includes destination IP addresses, port identifiers (such as
8 443 for HTTPS), and related connection and session attributes, including connection initiation
9 and termination timestamps, connection duration, and identifiers such as the protocol used (TCP
10 or UDP), the source IP address, the source port, the destination IP address, and the destination
11 port. The Third Parties use this information in real time to identify and log the origin and
12 destination endpoints of Plaintiffs' and Website users' electronic communications and the
13 characteristics of those connections, separate from any substantive "message" or "contents"
14 carried at the higher-level Application layer.

15 **F. The Private Communications Collected are Valuable.**

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

23 122. The Private Communications tracked and collected through cookies on the
24 Websites are valuable to Defendant and Third Parties. Defendant uses this data to measure and
25 optimize marketing campaigns, evaluate website design and product placement, and target
26 specific users or groups of users with advertising. For example, Defendant can identify
27 California users who visit webpages related to particular products and then target those users
28

1 with advertisements for similar products both on the Website and across unrelated third-party
2 websites.

3 123. Data reflecting users' browsing activity allows Defendant to identify behavioral
4 patterns, preferences, and interests, relating to Defendant's products. At scale, this data enables
5 Defendant to assess trends across its brands and within the broader clothing and fashion market.
6 Defendant monetizes this data by leveraging it to user engagement, advertising effectiveness,
7 and overall revenue.

8 124. The value of the Private Communications tracked and collected by the Third
9 Parties using cookies on the Websites can be quantified. Legal scholars observe that "[p]ersonal
10 information is an important currency in the new millennium."⁵⁵ Indeed, "[t]he monetary value
11 of personal data is large and still growing, and corporate America is moving quickly to profit
12 from the trend." *Id.* "Companies view this information as a corporate asset and have invested
13 heavily in software that facilitates the collection of consumer information." *Id.*

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

18 126. By falsely representing consumers' ability to reject or opt out of non-strictly
19 necessary cookies, and by aiding, agreeing with, employing, permitting, or otherwise enabling
20 the Third Parties to collect users' Private Communications, Defendant unjustly enriches itself at
21 the expense of consumer privacy and autonomy. Defendant deprives consumers of the ability to
22 decide whether, and on what terms, their data may be monetized.

23 **PLAINTIFFS' EXPERIENCES**

24 **Plaintiff Estrella Eugenio**

25 127. Plaintiff Eugenio visited the Loft and Ann Taylor Websites to seek and obtain
26 information about Defendant's women's clothing and fashion products, while located in
27 California, on multiple occasions during the last four years. In particular, Plaintiff Eugenio

28 ⁵⁵ See Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004).

1 browsed the Websites for women's apparel, reviewed available colors, inventory, promotions,
2 and new arrivals, and sought information regarding fashion trends, outfit ideas, and product
3 styles. Plaintiff Eugenio navigated the Websites both by using the Websites' search tools to
4 search for particular products and by browsing product categories and related webpages.

5 128. Plaintiff Eugenio's visits to the Websites were consistent with a typical Website
6 user's visits seeking information about Defendant's products. Specifically, Plaintiff Eugenio is
7 not a consumer advocate, a "tester," or a compliance auditor that visited the Loft Website to test
8 or evaluate Defendant's privacy practices.

9 129. When Plaintiff Eugenio visited the Websites, each Website immediately detected
10 that she was a visitor in California and presented her with Defendant's popup cookie consent
11 banner, which provided the option to select the "Manage Preferences" link. Plaintiff Eugenio
12 viewed Defendant's representation on the popup cookie consent banner that, "Our website uses
13 cookies to personalize your experience. Under certain state laws, collection of data through third-
14 party cookies for targeted advertising and similar purposes may be considered a 'sale.' If you
15 wish to opt out of such a 'sale' of your personal information, please click Manage Preferences[.]
16 You may also use this tool to learn more about our use of cookies and set your preferences."
17 Plaintiff Eugenio also saw that the phrase "Manage Preferences" was a link that she could click
18 or select.

19 130. Plaintiff Eugenio selected and clicked the "Manage Preferences" link, which
20 caused Defendant's Cookie Preference Center to appear. There, Plaintiff Eugenio viewed
21 Defendant's additional representations that she could "opt out of certain cookies, including those
22 used for advertising purposes" by moving "the toggle switch next to the cookie name from Blue
23 (Active) to Gray (Inactive)." Plaintiff Eugenio saw Defendant's further representations that she
24 could opt out of or reject all cookies, including all Advertising and Functional cookies, other
25 than those strictly necessary for the Websites to function. Accordingly, Plaintiff Eugenio
26 adjusted the toggle switch from active to inactive for each category of Advertising and
27 Functional cookies, clicked or selected the "Save Settings" button on the Cookie Preference
28 Center, and proceeded to browse the Websites.

1 131. Plaintiff Eugenio believed that adjusting the toggle switches on the Cookie
2 Preference Center found on the Websites would allow her to opt out of, decline, and/or reject all
3 non-strictly necessary cookies and other tracking technologies (inclusive of those cookies that
4 cause the disclosure of tracking data to third-party advertising networks, analytics services,
5 and/or social media companies for the purposes of providing personalized content, targeted
6 advertising, and third-party services).

7 132. In adjusting the available toggle switches on the cookies preferences window,
8 Plaintiff Eugenio gave Defendant notice that she did not consent to the use or placement of
9 cookies and tracking technologies while browsing the Websites. Further, Plaintiff Eugenio
10 specifically rejected, based on Defendant's representations, those cookies used to "collect data
11 from visitors through cookies in order to personalize [the user] experience, including to serve
12 [users] targeted content and ads" and share information with third parties. In reliance on these
13 representations and promises, only then did Plaintiff Eugenio continue browsing the Websites.

14 133. Even before the popup cookie consent banner and Cookie Preference Center
15 appeared on the screen, Defendant nonetheless caused cookies and tracking technologies,
16 including those used for personalized content, targeted advertising, and providing third-party
17 services, to be placed on Plaintiff Eugenio's device and/or transmitted to the Third Parties along
18 with user data, without Plaintiff Eugenio's knowledge. Accordingly, the popup cookie consent
19 banner's and cookies preferences window's representations to Plaintiff Eugenio that she could
20 opt out of or reject the use and/or placement of all categories cookies and tracking technologies,
21 including all Advertising and Functional cookies, other than those strictly necessary for the
22 Websites to function, while she browsed the Websites was false. Contrary to what Defendant
23 made Plaintiff Eugenio believe, she did not have a choice about whether third-party cookies
24 would be placed on her device and/or transmitted to the Third Parties along with her user data;
25 rather, Defendant had already caused that to happen.

26 134. Then, as Plaintiff Eugenio continued to browse the Websites in reliance on the
27 promises Defendant made in the cookie consent banner and cookies preferences window, and
28 despite Plaintiff Eugenio's clear rejection of the use and/or placement of such cookies and

1 tracking technologies, Defendant nonetheless continued to cause the placement and/or
2 transmission of cookies along with user data, including those involved in providing personalized
3 content, targeted advertising, and third-party services from the Third Parties on her device. In
4 doing so, Defendant permitted the Third Parties to track and collect Plaintiff Eugenio's Private
5 Communications as Plaintiff Eugenio browsed the Websites.

6 135. Defendant's representations that consumers could opt out of or reject all cookies,
7 including all Advertising and Functional cookies, other than those strictly necessary for the
8 Websites to function, while Plaintiff Eugenio and users browsed the Websites, or at least those
9 involved in providing personalized content, targeted advertising, and third-party services, were
10 untrue. Had Plaintiff Eugenio known this fact, she would not have used the Websites. Moreover,
11 Plaintiff Eugenio reviewed the popup cookie consent banner and Cookie Preference Center prior
12 to using the Websites. Had Defendant disclosed that it would continue to cause cookies and
13 tracking technologies to be stored on consumers' devices even after they choose to opt out of or
14 reject all cookies, including all Advertising and Functional cookies, other than those strictly
15 necessary for the Websites to function, Plaintiff Eugenio would have noticed it and would not
16 have used the Websites or, at a minimum, she would have interacted with the Websites
17 differently.

18 136. Plaintiff Eugenio continues to desire to browse content featured on the Websites.
19 Plaintiff Eugenio would like to browse websites that do not misrepresent that users can opt out
20 of or reject cookies and tracking technologies. If the Websites were programmed to honor users'
21 requests to opt out of or reject cookies and tracking technologies, Plaintiff Eugenio would likely
22 browse the Websites again in the future, but will not do so until then. Plaintiff Eugenio regularly
23 visits websites that feature content similar to that of the Websites. Because Plaintiff Eugenio
24 does not know how the Websites are programmed, which can change over time, and because she
25 does not have the technical knowledge necessary to test whether the Websites honor users'
26 requests to opt out of or reject all categories of cookies, including all Advertising and Functional
27 cookies, other than those strictly necessary for the Websites to function, Plaintiff Eugenio will
28 be unable to rely on Defendant's representations when browsing the Websites in the future absent

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

8 **Plaintiff Revital Yogev**

9 137. Plaintiff Yogev visited the Loft and Ann Taylor Websites to seek and obtain
10 information about Defendant’s women’s clothing and fashion products, while located in
11 California, on multiple occasions during the last four years. In particular, Plaintiff Yogev
12 browsed the Websites for women’s apparel, including tops, pants, jackets, and accessories,
13 reviewed available colors, inventory, promotions, and new arrivals, and sought information
14 regarding fashion trends, outfit ideas, and product styles. Plaintiff Yogev navigated the Websites
15 both by using the Websites’ search tools to search for particular products and by browsing
16 product categories and related webpages.

17 138. Plaintiff Yogev’s visits to the Websites were consistent with a typical Website
18 user’s visits seeking information about Defendant’s products. Specifically, Plaintiff Yogev is not
19 a consumer advocate, a “tester,” or a compliance auditor that visited the Websites to test or
20 evaluate Defendant’s privacy practices.

21 139. When Plaintiff Yogev visited the Websites, the Websites immediately detected
22 that she was a visitor in California and presented her with Defendant’s popup cookie consent
23 banner, which provided the option to select the “Manage Preferences” link. Plaintiff Yogev
24 viewed Defendant’s representation on the popup cookie consent banner that, “Our website uses
25 cookies to personalize your experience. Under certain state laws, collection of data through third-
26 party cookies for targeted advertising and similar purposes may be considered a ‘sale.’ If you
27 wish to opt out of such a ‘sale’ of your personal information, please click Manage Preferences[.]
28 You may also use this tool to learn more about our use of cookies and set your preferences.”

1 Plaintiff Yogev also saw that the phrase “Manage Preferences” was a link that she could click or
2 select.

3 140. Plaintiff Yogev selected and clicked the “Manage Preferences” link, which
4 caused Defendant’s Cookie Preference Center to appear. There, Plaintiff Yogev viewed
5 Defendant’s additional representations that she could “opt out of certain cookies, including those
6 used for advertising purposes” by moving “the toggle switch next to the cookie name from Blue
7 (Active) to Gray (Inactive).” Plaintiff Yogev saw Defendant’s further representations that she
8 could opt out of or reject all categories of cookies, including all Advertising and Functional
9 cookies, other than those strictly necessary for the Websites to function. Accordingly, Plaintiff
10 Yogev adjusted the toggle switch from active to inactive for each category of Advertising and
11 Functional cookies, clicked or selected the “Save Settings” button on the Cookie Preference
12 Center, and proceeded to browse the Websites.

13 141. Plaintiff Yogev believed that adjusting the toggle switches on the Cookie
14 Preference Center found on the Websites would allow her to opt out of, decline, and/or reject all
15 non-necessary cookies and other tracking technologies (inclusive of those cookies that cause the
16 disclosure of tracking data to third-party advertising networks, analytics services, and/or social
17 media companies for the purposes of providing personalized content, targeted advertising, and
18 third-party services).

19 142. In adjusting the available toggle switches on the cookies preferences window,
20 Plaintiff Yogev gave Defendant notice that she did not consent to the use or placement of cookies
21 and tracking technologies while browsing the Websites. Further, Plaintiff Yogev specifically
22 rejected, based on Defendant’s representations, those cookies used to “collect data from visitors
23 through cookies in order to personalize [the user] experience, including to serve [users] targeted
24 content and ads” and share information with third parties. In reliance on these representations
25 and promises, only then did Plaintiff Yogev continue browsing the Websites.

26 143. Even before the popup cookie consent banner and Cookie Preference Center
27 appeared on the screen, Defendant nonetheless caused cookies and tracking technologies,
28 including those used for personalized content, targeted advertising, and providing third-party

1 services, to be placed on Plaintiff Yogev's device and/or transmitted to the Third Parties along
2 with user data, without her knowledge. Accordingly, the popup cookie consent banner's and
3 cookies preferences window's representations to Plaintiff Yogev that she could reject the use
4 and/or placement of all categories cookies and tracking technologies, including all Advertising
5 and Functional cookies, other than those strictly necessary for the Websites to function, while
6 she browsed the Websites was false. Contrary to what Defendant made Plaintiff Yogev believe,
7 she did not have a choice about whether third-party cookies would be placed on her device and/or
8 transmitted to the Third Parties along with her user data; rather, Defendant had already caused
9 that to happen.

10 144. Then, as Plaintiff Yogev continued to browse the Websites in reliance on the
11 promises Defendant made in the cookie consent banner and cookies preferences window, and
12 despite her clear rejection of the use and/or placement of such cookies and tracking technologies,
13 Defendant nonetheless continued to cause the placement and/or transmission of cookies along
14 with user data, including those involved in providing personalized content, targeted advertising,
15 and third-party services from the Third Parties on her device. In doing so, Defendant permitted
16 the Third Parties to track and collect Plaintiff Yogev's Private Communications as she browsed
17 the Websites.

18 145. Defendant's representations that consumers could reject all categories of cookies,
19 including all Advertising and Functional cookies, other than those strictly necessary for the
20 Websites to function, while Plaintiff Yogev and users browsed the Websites, or at least those
21 involved in providing personalized content, targeted advertising, and third-party services, were
22 untrue. Had Plaintiff Yogev known this fact, she would not have used the Websites. Moreover,
23 Plaintiff Yogev reviewed the popup cookie consent banner and Cookie Preference Center prior
24 to using the Websites. Had Defendant disclosed that it would continue to cause cookies and
25 tracking technologies to be stored on consumers' devices even after they choose to reject all
26 cookies, including all Advertising and Functional cookies, other than those strictly necessary for
27 the Websites to function, Plaintiff Yogev would have noticed it and would not have used the
28 Websites or, at a minimum, she would have interacted with the Websites differently.

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

CLASS ALLEGATIONS

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

Class: All persons who browsed any of the Websites in the State of California after rejecting all non-strictly necessary cookies in the Website's cookies preferences window.

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

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

5 150. **Common Questions Predominate:** This action involves common questions of
6 law and fact to the Class because each class member's claim derives from the same unlawful
7 conduct that led them to believe that Defendant would not cause third-party cookies to be placed
8 on their browsers and devices and/or transmitted to third parties along with user data, after Class
9 members chose to reject all non-strictly necessary cookies and tracking technologies (including
10 Advertising and Functional cookies) on the Websites, nor would Defendant permit third parties
11 to track and collect Class members' Private Communications as Class members browsed the
12 Websites.

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

- 16 a. Whether Defendant's actions violate California laws invoked herein; and
17 b. Whether Plaintiffs and Class members are entitled to damages, restitution,
18 injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest and costs
19 of this suit.

20 152. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of
21 the Class because, among other things, Plaintiffs, like the other Class members, visited Websites,
22 rejected non-strictly necessary cookies, and had their confidential Private Communications
23 intercepted by the Third Parties.

24 153. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the
25 interests of all Class members because it is in their best interest to prosecute the claims alleged
26 herein to obtain full compensation due to them for the unfair and illegal conduct of which they
27 complain. Plaintiffs also have no interests in conflict with, or antagonistic to, the interests of
28 Class members. Plaintiffs have retained highly competent and experienced class action attorneys

1 to represent their interests and those of the Class. By prevailing on their claims, Plaintiffs will
2 establish Defendant's liability to all Class members. Plaintiffs and their counsel have the
3 necessary financial resources to adequately and vigorously litigate this class action, and Plaintiffs
4 and counsel are aware of their fiduciary responsibilities to the Class members and are determined
5 to diligently discharge those duties by vigorously seeking the maximum possible recovery for
6 Class members.

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

20 **CAUSES OF ACTION**

21 **First Cause of Action: Invasion of Privacy**

22 155. Plaintiffs reallege and incorporate the paragraphs of this Complaint as if set forth
23 herein.

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

27 157. Defendant has intruded upon the following legally protected privacy interests of
28 Plaintiffs and Class members: (i) the California Invasion of Privacy Act, as alleged herein;

(ii) the California Constitution, which guarantees Californians the right to privacy; (iii) the California Wiretap Acts as alleged herein; (iv) Cal. Penal Code § 484(a), which prohibits the knowing theft or defrauding of property “by any false or fraudulent representation or pretense;” and (v) Plaintiffs’ and Class members’ Fourth Amendment right to privacy.

158. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as Defendant affirmatively promised users they could opt out of all non-strictly necessary cookies and tracking technologies (including Advertising and Functional cookies), before proceeding to browse the Websites. Plaintiffs and other Class members directed their electronic devices to access the Websites and, when presented with the popup cookies consent banner and Cookie Preference Center on the Websites, Plaintiffs and Class members opted out of or rejected all such cookies and reasonably expected that their rejection of such cookies and tracking technologies would be honored. That is, they reasonably believed that Defendant would not permit the Third Parties to store and send cookies and/or use other such tracking technologies on their devices while they browsed the Websites. Plaintiffs and Class members also reasonably expected that, if they opted out of non-strictly necessary cookies and/or tracking technologies, Defendant would not permit the Third Parties to track and collect Plaintiffs’ and Class members’ Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, on the Websites.

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

160. Defendant, in violation of Plaintiffs’ and other Class members’ reasonable expectation of privacy and without their consent, permits the Third Parties to use cookies and other tracking technologies to collect, track, and compile users’ Private Communications, including their browsing history, visit history, website interactions, user input data, demographic

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

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

17 162. Defendant’s intrusion into Plaintiffs’ privacy was also highly offensive to a
18 reasonable person.

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

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

27 165. Plaintiffs and Class members seek appropriate relief for that injury, including but
28 not limited to, damages that will compensate them for the harm to their privacy interests as well

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

3 166. Plaintiffs and Class members seek punitive damages because Defendant's
4 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and
5 Class members and made in conscious disregard of Plaintiffs' and Class members' rights and
6 Plaintiffs' and Class members' rejection of the Websites' use of non-strictly necessary cookies
7 (including Advertising and Functional cookies). Punitive damages are warranted to deter
8 Defendant from engaging in future misconduct.

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

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

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

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

24 170. The Third Parties' tracking and collecting of Plaintiffs' and Class member's
25 Private Communications on the Websites using third-party cookies that Defendant caused to be
26 stored on users' devices—and to be transmitted to Third Parties—was not authorized by
27 Plaintiffs and Class members, and, in fact, those Websites' users specifically chose to opt out of
28

1 all cookies, including all Advertising and Functional cookies, other than those strictly necessary
2 for the Websites to function.

3 171. Plaintiffs and the Class members had an objectively reasonable expectation of
4 privacy surrounding their Private Communications on the Websites based on Defendant's
5 promise that users could opt out of all cookies, including all Advertising and Functional cookies,
6 other than those strictly necessary for the Websites to function, as well as state criminal and civil
7 laws designed to protect individual privacy.

8 172. Defendant's intentional intrusion into Plaintiffs' and other users' Private
9 Communications would be highly offensive to a reasonable person given that Defendant
10 represented that its Websites' users could opt out of all cookies, including all Advertising and
11 Functional cookies, other than those strictly necessary for the Websites to function, when, in
12 fact, Defendant caused such third-party cookies to be stored on consumers' devices and
13 browsers, and to be transmitted to third parties, even when consumers opted out of or rejected
14 all such cookies. Indeed, Plaintiffs and Class members reasonably expected, based on
15 Defendant's false representations, that when they opted out of all such cookies and tracking
16 technologies, Defendant would not cause such third-party cookies to be stored on their devices
17 or permit the Third Parties to obtain their Private Communications on the Websites, including
18 their browsing history, visit history, website interactions, user input data, demographic
19 information, interests and preferences, shopping behaviors, device information, referring URLs,
20 session information, user identifiers, and/or geolocation data—including whether a user is
21 located in California.

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

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

26 175. Plaintiffs and Class members seek appropriate relief for that injury, including but
27 not limited to, damages that will compensate them for the harm to their privacy interests as well
28

as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs’ and Class members’ privacy.

176. Plaintiffs and Class members seek punitive damages because Defendant’s actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs’ and Class members’ rights and Plaintiffs’ and Class members’ rejection of the Websites’ use of non-strictly necessary cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

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

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

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

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

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

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

181. Each of the Third Parties is a separate legal entity that offers a software-as-a-service and not merely a passive device. Further, the Third Parties had the capability to use the wiretapped information for their own purposes and, as alleged above, they did in fact use the wiretapped information for their own business purposes. Accordingly, the Third Parties were

1 third parties to any communication between Plaintiffs and Class members, on the one hand, and
2 Defendant, on the other.

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

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

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

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

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

4 187. Plaintiffs and Class members did not provide their prior consent to the Third
5 Parties' intentional access, interception, reading, learning, recording, collection, and usage of
6 Plaintiffs' and Class members' electronic communications. Nor did Plaintiffs and Class
7 members provide their prior consent to Defendant aiding, agreeing with, employing, permitting,
8 or otherwise enabling the Third Parties' conduct. On the contrary, Plaintiffs and Class members
9 expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept,
10 read, learn, record, collect, and use Plaintiffs' and Class members' electronic communications
11 by choosing to opt out of all non-strictly necessary cookies in the Websites' Cookie Preference
12 Center.

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

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

27 190. Pursuant to California Penal Code § 637.2, Plaintiffs and Class members have
28 been injured by the violations of California Penal Code § 631, and each seeks statutory damages

of the greater of \$5,000, or three times the amount of actual damages, for each of Defendant's violations of CIPA § 631(a), as well as injunctive relief.

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

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

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

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

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

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

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

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

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

17 198. Some of the information collected by the Third Parties’ cookies and the
18 corresponding software, including IP addresses and user-agent information, does not constitute
19 the content of Plaintiffs’ and the Class members’ electronic communications with the Websites.

20 199. Plaintiffs and Class members did not provide their prior consent to Defendant’s
21 use of third-party cookies and the corresponding software. On the contrary, Plaintiffs and the
22 Class members informed Defendant that they did not consent to the Websites’ use of third-party
23 cookies by adjusting the available toggle switches to the inactive position on the cookies
24 preferences window.

25 200. Defendant did not obtain a court order to install or use the third-party cookies and
26 corresponding software to track and collect Plaintiffs’ and Class member’s IP addresses and
27 user-agent information.
28

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

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

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

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

204. Defendant fraudulently and deceptively informed Plaintiffs and Class members that they could reject all non-strictly necessary cookies (including Advertising and Functional cookies).

205. However, despite Defendant's representations otherwise, Defendant caused third-party cookies and software code to be stored on consumers' devices, and to be transmitted to the Third Parties alongside Private Communications, even after users adjusted the available toggle switches to the inactive position on the cookies preferences window. These cookies and corresponding software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' Private Communications, even when consumers had previously chosen to reject all such cookies.

206. These misrepresentations and omissions were known exclusively to, and actively concealed by Defendant, not reasonably known to Plaintiffs and Class members, and material at the time they were made. Defendant knew, or should have known, how the Websites functioned, including the Third Party's resources it installed on the Websites and the third-party cookies in use on the Websites, through testing the Websites, evaluating its performance metrics by means of its accounts with the Third Parties, or otherwise, and knew, or should have known, that the Websites' programming allowed the third-party cookies to be placed on users'—including Plaintiffs'—browsers and devices and/or transmitted to the Third Parties along with users' Private Communications even after users attempted to reject all non-strictly necessary cookies (including Advertising and Functional cookies), which Defendant promised its users they could do. Defendant's misrepresentations and omissions concerned material facts that were essential to the analysis undertaken by Plaintiffs and Class members as to whether to use the Websites. In

1 misleading Plaintiffs and Class members and not so informing them, Defendant breached its
2 duty to Plaintiffs and Class members. Defendant also gained financially from, and as a result of,
3 its breach.

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

6 208. Plaintiffs and Class members have suffered an injury-in-fact, including the loss
7 of money and/or property, as a result of Defendant's unfair, deceptive, and/or unlawful practices,
8 including the unauthorized interception of their Private Communications, including their
9 browsing history, visit history, website interactions, user input data, demographic information,
10 interests and preferences, shopping behaviors, device information, referring URLs, session
11 information, user identifiers, and/or geolocation data, which have value as demonstrated by the
12 use and sale of consumers' browsing activity, as alleged above. Plaintiffs and Class members
13 have also suffered harm in the form of diminution of the value of their private and personally
14 identifiable information and communications.

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

18 210. Defendant's representation that consumers could reject all non-strictly necessary
19 cookies, including all Advertising and Functional cookies, if they adjusted the available toggle
20 switches to the inactive position on the Cookie Preference Center was untrue. Again, had
21 Plaintiffs and Class members known these facts, they would not have used the Websites.
22 Moreover, Plaintiffs and Class members reviewed the popup cookie consent banner and Cookie
23 Preference Center prior to their interactions with the Websites. Had Defendant disclosed that it
24 caused third-party cookies to be stored on visitors' devices that are related to personalization,
25 targeted advertising, and third-party services, and/or share information with third parties, even
26 after they choose to reject all such cookies, Plaintiffs and Class members would have noticed it
27 and would not have interacted with the Websites.
28

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

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

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

214. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' choice to opt out of the Websites' use of all cookies, including all Advertising and Functional cookies, other than those strictly necessary for the Websites to function. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Sixth Cause of Action: Unjust Enrichment

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

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

217. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could opt out of all cookies, including all Advertising and Functional cookies, other than those strictly necessary for the Websites to function, and by permitting the Third Parties to store and transmit cookies on Plaintiffs' and Class members' devices and browsers, which permitted the Third Parties to track and collect users' Private

1 Communications, including their browsing history, visit history, website interactions, user input
2 data, demographic information, interests and preferences, shopping behaviors, device
3 information, referring URLs, session information, user identifiers, and/or geolocation data, even
4 after Class members opted out of or rejected all such cookies.

5 218. Plaintiffs and Class members' Private Communications have conferred an
6 economic benefit on Defendant.

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

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

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

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

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

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

24 **PRAYER FOR RELIEF**

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

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

1 B. An award of compensatory damages, including statutory damages where
2 available, to Plaintiffs and Class members against Defendant for all damages sustained as a result
3 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: May 22, 2026

14 **GUTRIDE SAFIER LLP**

15 /s/ Seth A. Safier

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

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

marie@gutridesafier.com

17 Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

18 100 Pine Street, Suite 1250

San Francisco, CA 94111

19 Telephone: (415) 639-9090

20 Facsimile: (415) 449-6469

21 *Attorneys for Plaintiffs*