UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

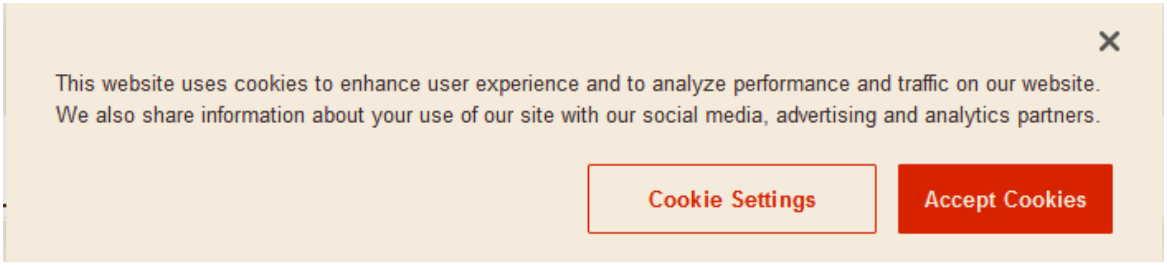
DANIEL PEMBERTON, an individual, on behalf of himself, the general public, and those similarly situated, Plaintiff, v. RESTAURANT BRANDS INTERNATIONAL, INC. and RESTAURANT BRANDS INTERNATIONAL US SERVICES LLC, Defendants.	CASE NO. CLASS ACTION COMPLAINT FOR INVASION OF PRIVACY; INTRUSION UPON SECLUSION; 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; UNJUST ENRICHMENT; AND TRESPASS TO CHATTELS JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiff Daniel Pemberton ("Plaintiff") brings this action on behalf of himself, the general public, and all others similarly situated against Restaurant Brands International, Inc. and Restaurant Brands International US Services LLC (collectively, "Defendants" or "Burger King"). Plaintiff's allegations against Defendants are based upon information and belief and upon investigation of Plaintiff's counsel, except for allegations specifically pertaining to Plaintiff, which are based upon Plaintiff's personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns an egregious privacy violation and total breach of consumer trust in violation of California law. When consumers visit Defendants' website (www.bk.com, the "Website"), Defendants display to them a popup cookie consent banner. Defendants' cookie banner discloses that the Website uses cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendants assure visitors that they do not have to "Accept Cookies," but can instead choose to manage their "Cookie Settings" as shown in the following screenshot:



2. Like most websites, Defendants designed the Website to include resources and programming scripts from third parties that cause those parties to place cookies and other similar tracking technologies on visitors' browsers and devices and to transmit cookies along with user data. However, unlike other websites, Defendants' Website offers consumers a choice to browse without being tracked, followed, and targeted by third party data brokers and advertisers. However, Defendants' promises are outright lies, designed to lull users into a false sense of security. Even after users elect to manage their "Cookie Settings" and opt out of the sale/sharing of their personal information and all cookies that were not strictly necessary, Defendants surreptitiously causes several third parties – including Google LLC (DoubleClick and Google

Analytics), Meta Platforms, Inc. (Facebook), Microsoft Corporation (Microsoft Clarity), Snap Inc. (SnapChat), The Trade Desk, Inc., and AdTheorent, Inc. (the "Third Parties") – to place and/or transmit cookies that track users' website browsing activities and eavesdrop on users' private communications on the Website.

3. Contrary to their rejection of cookies and tracking technologies on the Website, Defendants nonetheless caused cookies, including the Third Parties' cookies, to be sent to Plaintiff and other visitors' browsers, stored on their devices, and transmitted to the Third Parties along with user data. These third-party cookies permitted the Third Parties to track and collect data in real time regarding Website visitors' behaviors and communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

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

5. This type of tracking and data sharing is exactly what the Website visitors who elect to manage their "Cookie Settings" and opt out of all non-necessary cookies (including Targeting and Performance cookies) sought to avoid. Defendants falsely told Website users that it respected their privacy and that they could avoid tracking and data sharing when they browsed the Website. Despite receiving notice of consumers' express declination of consent, Defendants defied it and violated state statutes and tort duties.

THE PARTIES

6. Plaintiff Daniel Pemberton is, and was at all relevant times, an individual and resident of Antioch, California. Plaintiff intends to remain in California and makes his permanent home there.

7. Restaurant Brands International, Inc. is a Canadian corporation with its headquarters and principal place of business in Toronto, Canada.

8. Restaurant Brands International US Services LLC is a Florida limited liability corporation with its headquarters in Miami, Florida. Restaurant Brands International US Services LLC is a subsidiary of Restaurant Brands International, Inc.

9. The Parties identified in paragraphs 7-8 of this Class Action Complaint are collectively referred to hereafter as "Defendants."

10. At all times herein mentioned, each of the Defendants was the agent, servant, representative, officer, director, partner or employee of the other Defendants and, in doing the things herein alleged, was acting within the scope and course of his/her/its authority as such agent, servant, representative, officer, director, partner or employee, and with the permission and consent of each Defendants.

11. At all times herein mentioned, each of the Defendants was a member of, and engaged in, a joint venture, partnership and common enterprise, and acted within the course and scope of, and in pursuance of, said joint venture, partnership and common enterprise.

12. At all times herein mentioned, the acts and omissions of each of the Defendants concurred and contributed to the various acts and omissions of each and all of the other Defendants in proximately causing the injuries and damages as herein alleged.

13. At all times herein mentioned, each of the Defendants ratified each and every act or omission complained of herein.

14. At all times herein mentioned, each of the Defendants aided and abetted the acts and omissions of each and all of the other Defendants in proximately causing the damages, and other injuries, as herein alleged.

JURISDICTION AND VENUE

15. 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 Plaintiff and Defendants are citizens of different states.

16. The injuries, damages and/or harm upon which this action is based, occurred or arose out of activities engaged in by Defendants within, affecting, and emanating from, the State of California. Defendants regularly conduct and/or solicit 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. Defendants have engaged, and continues to engage, in substantial and continuous business practices in the State of California.

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

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

SUBSTANTIVE ALLEGATIONS

A. Defendants Programmed the Website to Include Third-Party Resources that Utilize Cookies and Tracking Technologies.

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

20. An IP address (Internet Protocol address) is a unique numerical label assigned to each device connected to a network that uses the Internet Protocol for communication, typically

expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4 addresses). IP addresses can identify the network a device is on and the specific device within that network. Public IP addresses used for internet-facing devices reveal geographical locations, such as country, city, or region, through IP geolocation databases.

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

22. The Website causes users' devices to store and/or transmit both first-party and third-party tracking cookies. Cookies are small text files sent by a website server to a user's web browser and stored locally on the user's device. As described below, cookies generally contain a unique identifier which causes the website to recognize and differentiate individual users. Cookie files are sent back to the website server along with HTTP requests, causing 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., facebook.com; analytics.google.com; and snapchat.com, etc.). When the user's browser loads a webpage (such as a webpage of the Website) containing embedded third-party resources, the third-parties' programming scripts typically determine whether the third-party cookies are already stored on the user's device and cause the user's browser to store those cookies on the device if they do not yet exist. Third-party cookies include an identifier that allows the third-

party to recognize and differentiate individual users across websites (including the Website) and across multiple browsing sessions.

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

- **Browsing History**: Information about the webpages a Website user visits, including the URLs, titles, and keywords associated with the webpages viewed, time spent on each page, and navigation patterns;
- **Visit History**: Information about the frequency and total number of visits to the Website;
- **Website Interactions:** Data on which links, buttons, or ads on the Website that a user clicks;
- **User Input Data**: The information the user entered into the Website's form fields, including search queries, the user's name, age, gender, email address, location, and/or payment information;
- **Demographic Information**: Inferences about age, gender, and location based on browsing habits and interactions with Website content;
- **Interests and Preferences**: Insights into user interests based on the types of Website content viewed, products searched for, or topics engaged with;
- **Shopping Behavior**: Information about the Website products viewed or added to shopping carts;
- **Device Information**: Details about the Website user's device, such as the type of device (mobile, tablet, desktop), operating system, and browser type;
- **Referring URL**: Information about the website that referred the user to the Website;

- **Session Information**: Details about the user's current Website browsing session, including the exact date and time of the user's session, the session duration and actions taken on the Website during that session;
- **User Identifiers**: A unique ID that is used to recognize and track a specific Website user across different websites over time; and/or
- **Geolocation Data**: General location information based on the Website user's IP address or GPS data, if accessible.

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

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

27. Defendants own several fast food restaurant brands, including Burger King. Defendants also own and operate the Website, which allows visitors to receive information about their menu items, offers, and purchase food for pickup or delivery. As they interact with the Website (e.g., by entering data into forms, clicking on links, and making selections), Website users communicate Private Communications to Defendants, 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.

28. Defendants chose to install or integrate the Website with resources from the Third Parties that, among other things, use cookies. Thus, when consumers visit the Website, both first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is caused by software code that Defendants incorporate into the Website, or that Defendants cause to be loaded. Because Defendants control the software code of the Website, they have complete control over whether first-party and third-party cookies are placed on Website users' devices and/or transmitted to third parties.

29. Defendants explained the reason that they use third-party cookies on the Website as follows in the cookie consent preferences window:

> We may use personal information to support "targeted advertising," "selling," or "sharing" of personal information, as defined by applicable privacy laws, which may result in third parties receiving your personal information.[1]

30. Further, Defendants explained the reasons they use "Targeting Cookies" on the Website in the cookie consent preferences window:

> Targeting cookies are used to understand user behavior across our websites. These cookies are also used to show ads that are more relevant to your interests. We may share this information with advertising platforms to help us display the most relevant messages to you. These cookies may also store information on user behavior obtained their browsing habits, which allows us to develop a specific profile and display advertisements appropriate to your profile.

Id.

31. Defendants also provided information about their use of third-party cookies on the Website in their Privacy Policy.[2] In Section 3, titled "Sharing of Information," Defendants provide the following "information about entities with which we may share your Personal Information:"

[1] Burger King's cookie consent preference window as it was available when Plaintiff opted out of cookies and tracking technologies on the Website.

[2] Burger King Privacy Policy (updated December 22, 2022) (current version available at https://www.bk.com/privacy-policy) (the "Privacy Policy"). Defendants have subsequently updated their Privacy Policy but, based on information and belief, this version was in effect when Plaintiff opted out of cookies and tracking technologies on the Website.

> Third-Party Companies that Provide Advertising. Some of the advertising on our Services may be provided by third parties, such as our advertisers. These companies may collect or receive certain information about your use of the Services, including through the use of cookies, beacons, and similar technologies, and this information may be combined with information collected across different websites and online services in order to deliver ads that are more relevant to you, both on and off our Services.

Privacy Policy, Section 3.

32. Defendants provided additional information about their use of third-party cookies on the Website in Section 4 ("Your Choices and Opt Out") of their Privacy Policy:

> We may use third parties to serve advertisements on our Services and on other websites and digital platforms. These companies may use cookies, web beacons or other technologies to report certain information about your visits to our Services and other websites in order to measure the effectiveness of our marketing campaigns and to deliver ads that are more relevant to you, both on and off our Services. We may also use services provided by service providers to serve targeted ads to you and others on such platforms.
>
> Cookies and Beacons. We and other companies that provide advertising and other services on our Services may use cookies and beacons to facilitate administration and navigation, to better understand and improve our Services, to determine and improve the advertising shown to you here or elsewhere, and to provide you with a customized online experience.
>
> "Cookies" are small files that are placed on your computer when you visit a website. Cookies may be used to store a unique identification number tied to your computer or device so that you can be recognized as the same user across one or more browsing sessions, and across one or more sites.
>
> ...
>
> "Beacons" (or "pixels") are technologies that communicate information from your device to a server. Beacons can be embedded in online content, videos, and emails, and can allow a server to read certain types of information from your device, know when you have viewed particular content or a particular email message, determine the time and date on which you viewed the beacon, and the IP address of your device.
>
> Beacons. We, along with third parties, also may use technologies called beacons (or "pixels") that communicate information from your device to a server. Beacons can be embedded in online content, videos, and emails, and can allow a server to read certain types of information from your device, know when you have viewed particular content or a particular email message, determine the time and date on which you viewed the beacon, and the IP address of your device. We and third parties use beacons for a variety of purposes, including to analyze the use of our

> Services and (in conjunction with cookies) to provide content and ads that are more relevant to you both on and off the Service.

Privacy Policy, Section 4.

33. Finally, in Section 6 ("Your California Privacy Rights") in the Privacy Policy, Defendants explain the following:

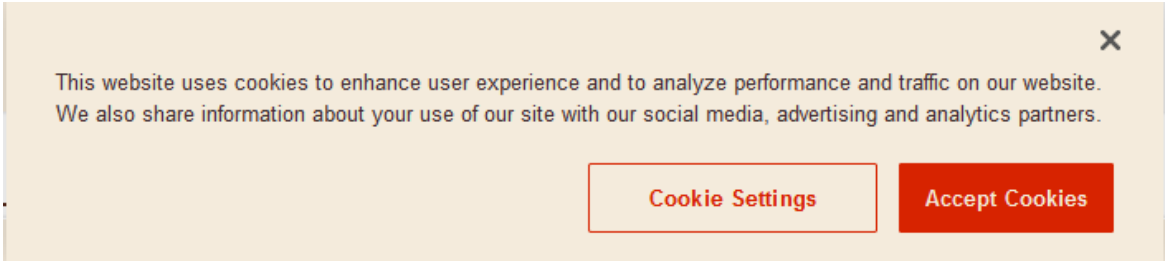
> Sale or Sharing of Personal Information. We do not sell your Personal Information in exchange for monetary compensation. We may disclose your Personal Information by allowing certain third parties to collect Personal Information via automated technologies on our websites for cross-context behavioral advertising purposes or other advertising, marketing, or analytics purposes. Under California law, these kinds of disclosures may be considered a "sale" when the Personal Information is exchanged for non-monetary consideration, or "sharing" when the Personal Information is disclosed for cross-context behavioral advertising purposes. You have the right to opt out of these types of disclosures of your information.
>
> We may sell or share for cross-context behavioral advertising purposes (and may have sold or shared during the 12-month period prior to the effective date of this Privacy Policy) the following categories of Personal Information about you to the following categories of third parties:
>
> - Identifiers/Contact Information, sold to/shared with social media platforms;
> - Commercial Information, sold to/shared with social media platforms, data analytics providers and business partners;
> - Internet/Electronic Network Activity, sold to/shared with social media platforms, data analytics providers, online advertising platforms, and business partners;
> - Geolocation Data, sold to/shared with data analytics providers and business partners;
> - Inferences, sold to/shared with social media platforms, data analytics providers and business partners.

Privacy Policy, Section 6.

B. <u>Defendants Falsely Informed Users That They Could Opt Out of the</u>

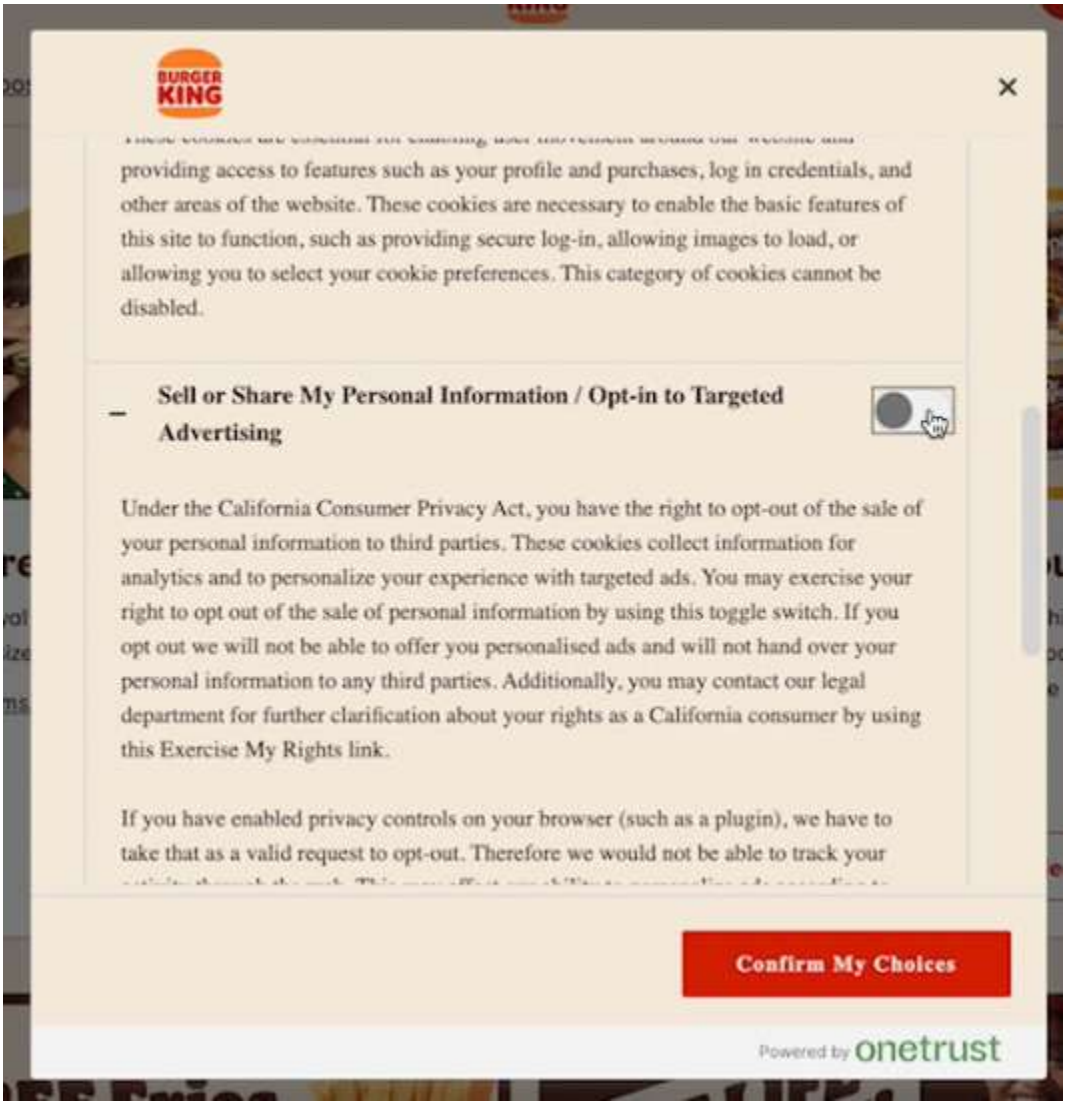
Website's Use of Cookies.

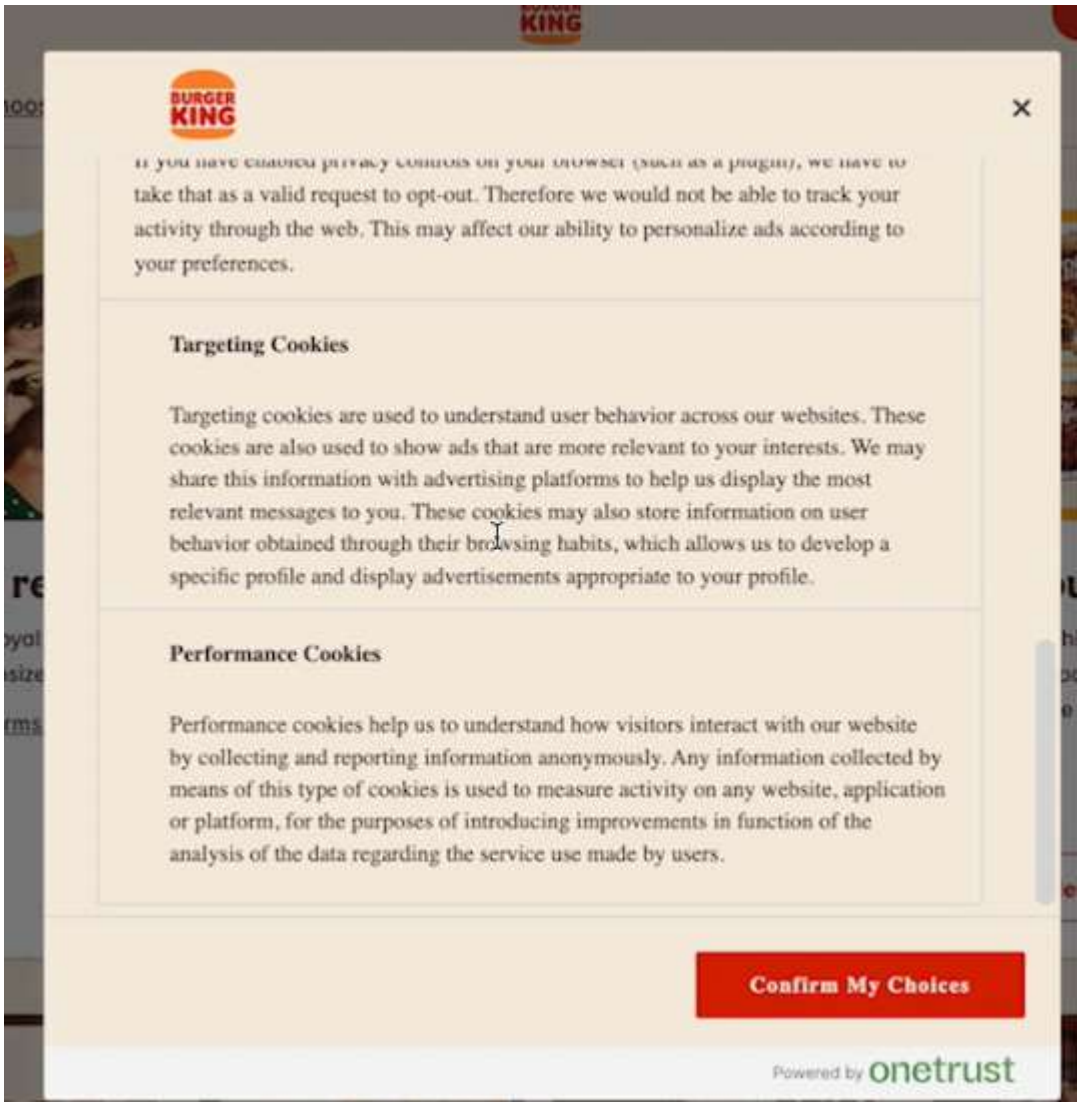
34. When consumers in California visited the Website, the Website immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the cookie consent banner stated, "This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising, and analytics partners." The banner then provided users the opportunity to accept cookies or manage "Cookie Settings" as shown, in the following screenshot from the Website:



35. Website users who click on the "Cookie Settings" button are presented with the cookie consent preferences window depicted in the screenshot below. The window represented to users that they could "move the toggle below to the [left/right] to opt out of [targeted advertising] activities on this digital property consistent with applicable law.

36. When a user clicks on the "+" sign to the left of the "Sell or Share My Personal Information / Opt-in to Targeted Advertising" header, the user is shown the information in the screenshots below. In particular, Defendants represented to consumers that "You may exercise your right to opt out of the sale of personal information by using this toggle switch. If you opt out we will not be able to offer you personalised ads and will not hand over your personal information to any third parties."





37. After users moved the toggle to the left, indicating their choice and/or agreement to opt out of the sale/sharing of their personal information and opt out of all cookies, except those that were strictly necessary, including targeting cookies and performance cookies, and clicked "Confirm My Choices," users could then continue to browse the Website, and the popup cookie consent banner and cookie consent preferences window disappeared.

38. Defendants' popup cookie consent banner and cookie consent preferences window led Plaintiff, and all those Website users similarly situated, to believe that they opted out of the sale/sharing of their personal information and opted out of all cookies, except those

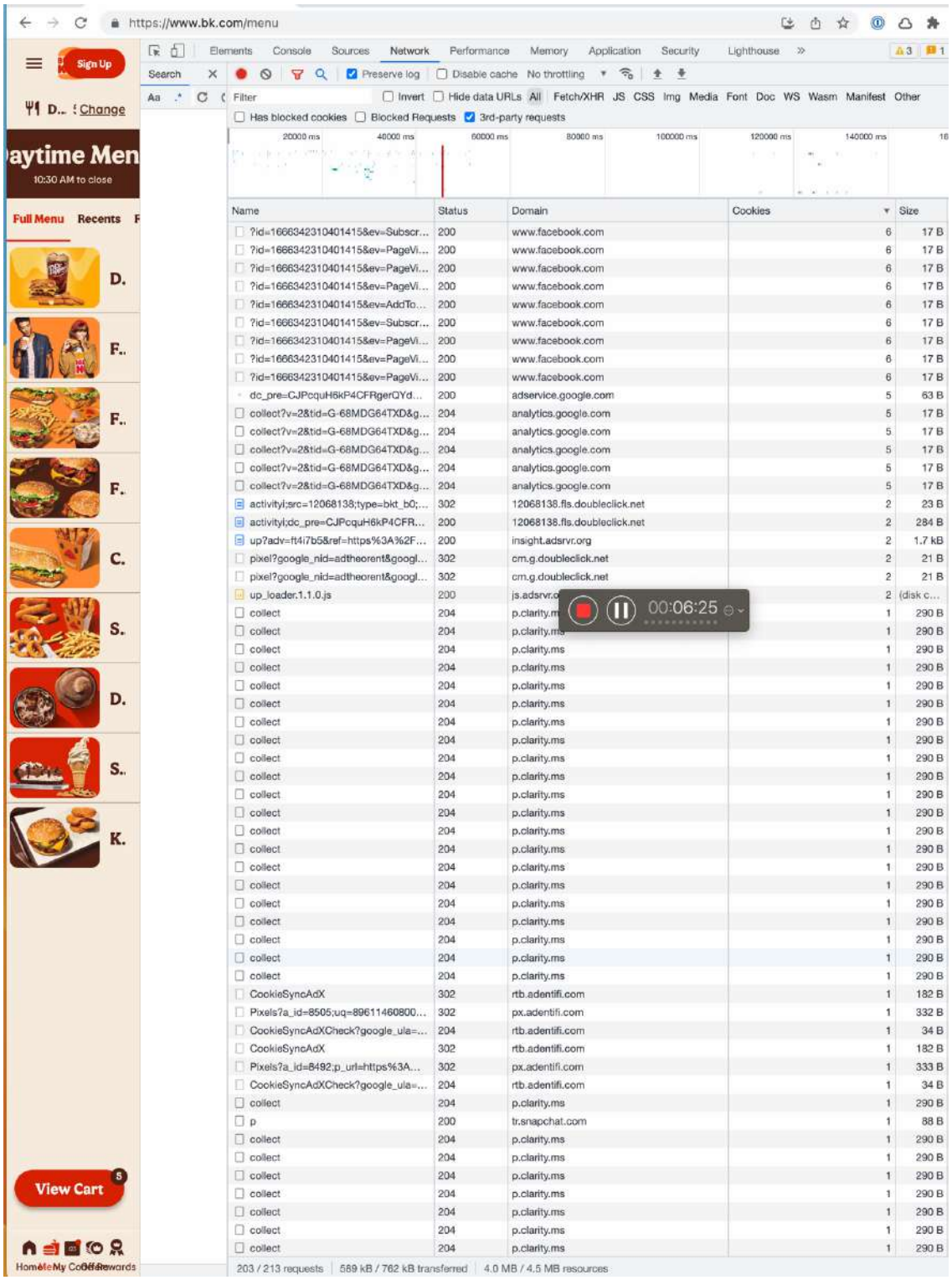
that were strictly necessary, including targeting cookies and performance cookies. The banner and preference window further reasonably led Plaintiff and those Website users similarly situated to believe that Defendants would not allow third parties, through cookies, to access their Private Communications with the Website, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, upon toggling off the sale/sharing of their personal information.

39. Defendants' representations, however, were false. In truth, Defendants did not abide by their users' wishes. When users moved the toggle to opt out of the sale/sharing of their personal information and opt out of all cookies, except those that were strictly necessary, including targeting cookies and performance cookies, they provided notice to Defendants that they did not consent to the placement or transmission of third-party cookies that would allow those parties to obtain their Private Communications with the Website. Nevertheless, Defendants caused the Third Party cookies to be placed on Website users' browsers and devices and/or to be transmitted to the Third Parties along with user data.

40. In particular, when users moved the toggle to opt out of the sale/sharing of their personal information and opt out of all cookies, except those that were strictly necessary, including targeting cookies and performance cookies, Defendants nonetheless continued to cause the Third Parties' cookies to be placed on users' devices and/or transmitted to the Third Parties along with user data, causing them to collect user data in real time that discloses Website visitors' Private Communications, including browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. In other words, even when consumers like Plaintiff tried to protect their privacy by rejecting cookies, Defendants failed to prevent cookies from being transmitted to Third Parties, causing them to track user behavior and communications.

41. Some aspects of the operations of the Third Party cookies on the Website can be observed using specialized tools that log incoming and outgoing Website network transmissions. The following screenshots, obtained using one such tool, show examples of Third-Party cookies being transmitted from a Website user's device and browser to Third Parties even after the user opted out of the sale/sharing of their personal information and opted out of all non-necessary cookies, including targeting cookies and performance cookies.

[REMAINDER OF PAGE INTENTIONALLY BLANK]



42. The screenshot above shows the "Network" tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user's browser and various third party websites while the user visited and interacted with the Website at

https://www.bk.com. The screenshot depicts only network traffic occurring ***after*** the user rejected all cookies using the cookie banner and cookie consent preference center. As shown above, despite the user's rejection of all cookies, the user's interactions with the Website resulted in the user's browser making a large number of GET and POST HTTP requests to third party web domains like facebook.com; analytics.google.com; and snapchat.com and others. As further shown in the right-hand column of the screenshot, the user's browser sent cookies along with those HTTP requests to the third parties. This screenshot demonstrates that the Website caused third-party cookie data and users' Private Communications to be transmitted to the Third Parties, even after consumers declined or rejected all cookies and tracking technologies by clicking or selecting the manage "Cookie Settings" button and opting out of the sale/sharing of their personal information and opting out of all cookies, except those that were strictly necessary, including targeting cookies and performance cookies. All of these network calls are made to the Third Parties without the user's knowledge, and despite the user's opt out of all cookies.

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

44. As users interact with the Website, even after opting out of the sale/sharing of their personal information and opting out of all cookies, except those that were strictly necessary, including targeting cookies and performance cookies, thereby declining or rejecting the use of cookies and similar technologies that cause the disclosure of user data to third-party social media, advertising, and analytics companies, as well as the sale or sharing of the user's personal information with third parties for such functions, or other purposes, more data regarding users' behavior and communications are sent to third parties, alongside the cookie data. The third-party cookies that Defendants wrongfully allow to be stored on users' devices and browsers, and to be

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

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

C. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting the Website.

1. Google Cookies

46. Defendants cause third party cookies to be transmitted to and from Website users' browsers and devices, even after users opt out of all non-required cookies (including targeting and performance cookies) to and from the **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 enable its advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Google's ad network.[5]

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

[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.

[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=11962135750754589 08-NC).

[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=11962135750754589 08-NC); *see also* Cookies and user identification (available at https://developers.google.com/tag-platform/security/concepts/cookies).

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

49. Google's cookies allow it to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data.[9]

50. The Google software code that Defendants cause to be stored on and executed by the Website user's device causes data to be sent to Google's domain, at https://analytics.google.com/g/collect. For example:

---

[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).

[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 (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).

Key	Value
v	2
tid	G-68MDG64TXD
gtm	45je3430
_p	794386311
cid	1480836074.1680636230
ul	en-us
sr	2240x1260
uaa	arm
uab	64
uafvl	Google%20Chrome;111.0.5563.146|Not(A%3ABrand;8.0.0.0|Chromium;111.0.5563.146
uamb	0
uam	
uap	macOS
uapv	13.2.1
uaw	0
_eu	AEA
dl	https://www.bk.com/menu
dr	https://www.bk.com/store-locator
sid	1680636229
sct	1
seg	1
dt	Main menu - Burger King
_s	5

51. The "cid" cookie above refers to "Client ID." It contains a unique identifier for the user's browser and device, that causes Google to link the user to their interactions with the website.[10] Further, in the example above, the value corresponding to the "dl" parameter indicates the URL that the user was visiting (i.e., https://www.bk.com/menu), whereas the value corresponding to the "dt" parameter indicates the title of the page (i.e., "Main menu – Burger King).

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

52. Along with this data, the Google software code that Defendants cause to be stored on and executed by the user's device causes cookies to be sent to the Google Analytics domain. For example:

Key	Value
__Secure-3PSID	VAjPknD0lAu0njG94lWPuI657X1-__D57Pn4bNvafL-U7GmaHiTNOTV32Rpzve9keknd1A.
__Secure-3PAPISID	hbGA11q3tl_WKoA0/A2Chlh7BWZm9M9hVi
1P_JAR	2023-04-04-19
NID	511=g5GZlyM9cHe07RGMLWTSoeT-DNj0L3KM-DgC89l9vu7akmjbdQgii1S2TBKXT5sD4irOGEPHkynfljqNGLBVgw7dyCz7AvQY71OmulrW-FcP2w7YSb4BodyzTU1u_OQLXi7lNJzlkdk2q1klocCQgw5Bq3vRhP8N3Kv9CJWlU7nXUB2HMwKfVqn7ET1Xz34YDGQs9r7eQqAn9b58JJqhxz9DVT0WAJGgD9nYx2rNTGD26w_HlNi9LeZnFHiujW9vtJJ7sLcztemzxeJCN0zU91HitT0B9YQYAix1JRpbLQYw6WCaVgHYA_sc2P3_35odP0sbmaBzYycrlJheP3U2uOkczTL_W8s-abPXLg
__Secure-3PSIDCC	AFvIBn9o85NWMTvj2iTFVc3VdApM8D7kzNw40aRX9qr4Qvufa0HQ6UZ2DtmfOZsgvYM0RDDfHFI

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

54. Similarly, the Google software code that Defendants cause to be stored on and executed by the user's device causes cookies to be sent to Google's advertising domain, at https://adservice.google.com. For example:

Key	Value
__Secure-3PSID	VAjPknD0lAu0njG94lWPuI657X1-__D57Pn4bNvafL-U7GmaHiTNOTV32Rpzve9keknd1A.
__Secure-3PAPISID	hbGA11q3tl_WKoA0/A2Chlh7BWZm9M9hVi
1P_JAR	2023-04-04-19
NID	511=g5GZlyM9cHe07RGMLWTSoeT-DNj0L3KM-DgC89l9vu7akmjbdQgii1S2TBKXT5sD4irOGEPHkynfljqNGLBVgw7dyCz7AvQY71OmulrW-FcP2w7YSb4BodyzTU1u_OQLXi7lNJzlkdk2q1klocCQgw5Bq3vRhP8N3Kv9CJWlU7nXUB2HMwKfVqn7ET1Xz34YDGQs9r7eQqAn9b58JJqhxz9DVT0WAJGgD9nYx2rNTGD26w_HlNi9LeZnFHiujW9vtJJ7sLcztemzxeJCN0zU91HitT0B9YQYAix1JRpbLQYw6WCaVgHYA_sc2P3_35odP0sbmaBzYycrlJheP3U2uOkczTL_W8s-abPXLg
__Secure-3PSIDCC	AFvIBn9o85NWMTvj2iTFVc3VdApM8D7kzNw40aRX9qr4Qvufa0HQ6UZ2DtmfOZsgvYM0RDDfHFI

55. As shown above, the values of the __Secure-3PSID, __Secure-3PAPISID, and __Secure-3PSIDCC cookies are the same values that were sent to Google's Analytics domain, further confirming Google's ability to link the user's data sent to Google Analytics with the data sent to Google's advertising domain.

56. Further, along with all of this data, the Google software code that Defendants cause to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to Google, at both the Google advertising and Google Analytics domains:

Key	Value
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

57. The "user-agent" corresponds to the device and browser that the user has used to access the Website. In this case, the user-agent value corresponds to Google's Chrome browser version 121, running on the Catalina version of macOS.[11]

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

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

60. Thus, the Google cookies used on the Website enable Google to (and Google does) track users' interactions with advertisements to help advertisers understand how users engage with ads across different websites. Further, the user data collected through the cookie

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

enables the delivery of personalized ads based on user interests and behaviors. For instance, if a user frequently visits travel-related websites, Google will show her more travel-related advertisements. Further, the collected data is used to generate reports for advertisers, helping them assess the performance of their ad campaigns and make data-driven decisions (such as renaming their products). Further, Google's advertising platform enables advertisers to retarget marketing, which Google explains allows advertisers to "show previous visitors ads based on products or services they viewed on your website. With messages tailored to your audience, dynamic remarketing helps you build leads and sales by bringing previous visitors back to your website to complete what they started."[12]

61. Further, in its "Shared Data Under Measurement Controller-Controller Data Protection Terms," Google states: "Google can access and analyze the Analytics data customers share with us to better understand online behavior and trends, and improve our products and services—for example, to improve Google search results, detect and remove invalid advertising traffic in Google Ads, and test algorithms and build models that power services like Google Analytics Intelligence that apply machine-learning to surface suggestions and insights for customers based on their analytics data and like Google Ads that applies broad models to improve ads personalization and relevance. These capabilities are critical to the value of the products we deliver to customers today."[13] Thus, Google can have the capability to use the data it collects for understanding online behavior and trends, machine learning, and improving its own products and services.

2. Meta Cookies

62. Defendants also cause third party cookies to be transmitted to and from Website users' browsers and devices to and from the **facebook.com** domain, even after users elect to reject all non-strictly necessary cookies (including Functional, Performance, Targeting, Social Media, and User Profile cookies). This domain is associated with Meta's digital advertising and

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

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

analytics platform that collects user information via cookies to assist Meta in performing data collection, behavioral analysis, user retargeting, and analytics.[14] Meta serves targeted ads to web users across Meta's ad network, which spans millions of websites and apps.

63. The facebook.com cookies help Meta track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. For example, the Website causes the following data to be sent to Meta when an "AddToCart" event is initiated:

Key	Value
id	1666342310401415
ev	AddToCart
dl	https://www.bk.com/menu/picker-eb542d84-a335-4991-afbc-94f232e5d325
rl	
if	false
ts	1680636476188
sw	2240
sh	1260
v	2.9.100
r	stable
ec	11
o	30
fbp	fb.1.1680636230058.1669038476
it	1680636229981
coo	false
rqm	GET

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

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

Key	Value
sb	uVYGZNaVuhf0oGmVlNsKLoRA
datr	uVYGZNelHg51fkvv9G6h4XWe
c_user	1345507951
dpr	2
xs	4%3AUWIuZLD5xjfNFg%3A2%3A1679357299%3A-1%3A2633%3A%3AAcXduiBF-JGEJ3wGQBvT9ExV67iKLCRS8Dn9taZgbg
fr	0pi8P6EtGtI9xHpGv.AWXjmhxpFzlQTh3weRFLDpTxns8.BkLHoA.MP.AAA.0.0.BkLHoA.AWVq5dxGb94

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

66. In particular, by identifying users who have shown interest in certain products or content, the facebook.com cookies enable Meta's advertising platform to cause advertisers to show relevant ads to those users when they visit other websites within Meta's ad network.[15] These cookies allow Meta to collect data on how users interact with websites, regardless of whether they have a Facebook account or are logged in.[16]

67. The facebook.com cookies allow Meta to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses).[17]

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

[16] https://allaboutcookies.org/what-data-does-facebook-collect.

[17] *Id.*

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

3. Microsoft Clarity Cookies

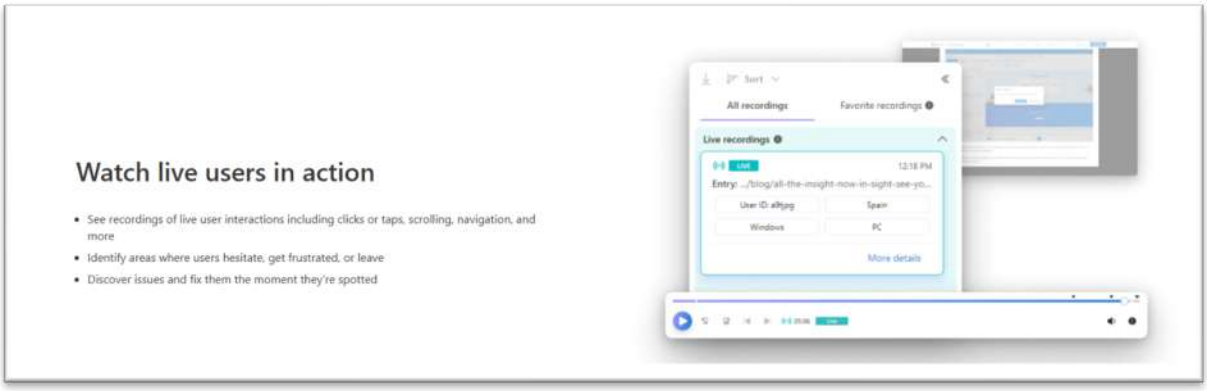
69. Even after users click or select the "Reject All" button to reject all cookies on the Website, Defendants cause cookies—along with ***recordings*** of user sessions—to be sent to Microsoft's **clarity.ms** domain. This domain is associated with Clarity, Microsoft's "cutting-edge behavioral analytics tool that helps you understand user interaction with your website or app".[18] Clarity is a Microsoft Advertising tool, which "crucial for successful marketing."[19] "Clarity's tracking code," like bat.bing.com, "uses a cookie to obtain user session data." [20]

[18] https://learn.microsoft.com/en-us/clarity/setup-and-installation/about-clarity.

[19] https://about.ads.microsoft.com/en/blog/post/october-2021/introducing-microsoft-clarity-insights-for-microsoft-advertising.

[20] https://learn.microsoft.com/en-us/clarity/setup-and-installation/cookie-consent.

70. Clarity enables Defendants to "watch live users in action" via "recordings of live user interactions" on the website, including a user's "clicks or taps, scrolling, navigation, and more."[21] Indeed, Clarity boasts that it "tracks all visitor clicks and scrolls on mobile, desktop, and tablet[.]" These "session recordings" track each and every consumer's individual actions on the website.[22]



71. Further, Clarity permits Defendants to aggregate individual users' session recordings into "heatmaps" for Defendants' financial gain. Heatmaps are "visualization tool[s]" aimed at "aggregat[ing] information about how users interact with the website." [23] This allows Defendants to "See at a glance which areas on [web site owner's] page drive the most engagement," a crucial element to increasing advertising revenue. [24] Clarity also permits Defendants to "track a specific subset of users," including tracking metrics like what browser users visited from, what type of device, the date, and more. Clarity even permits the use of specific "Clarity user ID[s]" which permits Clarity to track users across their devices, and identify when the same user visits multiple times to the website.[25] Businesses use Clarity to "make data-driven decisions" to "improve overall conversion rates" of clicks, engagement, or

[21] https://clarity.microsoft.com/session-recordings.

[22] https://clarity.microsoft.com/session-recordings.

[23] https://learn.microsoft.com/en-us/clarity/heatmaps/heatmaps-overview.

[24] https://clarity.microsoft.com/heatmaps.

[25] https://clarity.microsoft.com/insights; https://learn.microsoft.com/en-us/clarity/setup-and-installation/identify-api.

sales.[26] Microsoft notes in a Clarity case study that Clarity cookies permitted businesses to see a "substantial increase" in "purchases."[27] In one instance, "following just five days after implementing Clarity, the [business] saw an uplift of 19% in conversion rate."[28] Businesses consider Clarity a "must-have tool for any business serious about optimizing their website and increasing online revenue."[29]

72. Microsoft collects data from Clarity,[30] which "Microsoft retains . . . for as long as necessary[.]"[31] Clarity cookies allow Microsoft to obtain and store at least the following user data: (i) user identifier; (ii) website interactions; (iii) interests and preferences; (iv) shopping behavior; (v) device information; (vi) demographic data; (vii) geolocation data; (viii) referring URL; and (ix) session information. [32]

4. Additional Third Party Cookies

73. Defendants also cause third party cookies to be transmitted to and from Website users' browsers and devices, even after users elect to opt out of all non-required cookies, to and from other domains, including tr.snapchat.com; insight.adsvr.org; and adentifi.com.

74. The subdomain **tr.snapchat.com** is associated with Snap Inc. (SnapChat), a social media company that uses its cookies to measure users' conduct across distinct websites to help advertisers target ads.[33] SnapChat uses tr.snapchat.com to collect data on browsing history,

---

[26] https://clarity.microsoft.com/case-studies/ecommerce-boost/#:~:text=Using%20Clarity&text=By%20analyzing%20user%20sessions%20and,and%20improve%20overall%20conversion%20rates.

[27] *Id.*

[28] *Id.*, emphasis in original.

[29] https://clarity.microsoft.com/case-studies/ecommerce-boost/#:~:text=Using%20Clarity&text=By%20analyzing%20user%20sessions%20and,and%20improve%20overall%20conversion%20rates.

[30] https://www.microsoft.com/en-us/privacy/privacystatement.

[31] *Id.*

[32] https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-data.

[33] *See* https://snapdiscoveries.com/what-is-tr-snapchat-com-is-used-for.

choices, and interactions with advertisements.[34] This data helps Snapchat personalize ad content and track users across the internet.[35]

75. 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.[36] 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."[37] This data helps The Trade Desk personalize ad content and track users across the internet.[38]

76. 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."[39]

77. The domain **adentifi.com** is associated with AdTheorent, Inc., a digital advertising company that offers a digital ad-buying platform that causes businesses to plan, manage, optimize, and measure online advertising campaigns. [40] AdTheorent uses rtb.adentifi.com cookies to collect data users' "as a targeting component" for digital advertising."[41] This data helps AdTheorent personalize ad content and track users across the internet.

78. 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

---

[34] *Id.*

[35] *Id.*

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

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *See* https://adtheorent.com/about.

[41] AdTheorent, Inc. Form 10-K (filed March 12, 2024).

information, (v) interests and preferences, (vi) shopping behaviors, (vii) device information, (viii) referring URLs, (ix) session information, (x) user identifiers, and (xi) geolocation data.

D. The Private Communications Collected are Valuable.

79. The Private Communications that the Third Parties track and collect by way of the cookies on the Website are valuable to Defendants as well as the Third Parties. Defendants can use the data to create and analyze the performance of marketing campaigns, website design, product placement, and target specific users or groups of users for advertisements. For instance, if Defendants wanted to market certain of their fast food products to consumers, Defendants could use the data collected by the Third Parties to monitor users who visit webpages related to specific products, then advertise similar products to those particular users when they visit other webpages. The third-party cookies also enable Defendants to (and Defendant does) target online advertisements to users when they visit ***other*** websites, even those completely unrelated to Defendants and their products.

80. Data about users' browsing history enables Defendants to spot patterns in users' behavior on the Website and their interests in, among other things, Defendants' fast food products. On a broader scale, it causes Defendants to gain an understanding of trends happening across their brands and across the fast food market. All of this helps Defendants further monetize the Website and maximize revenue by collecting and analyzing user data.

81. The value of the Private Communications tracked and collected by the Third Parties using cookies on the Website can be quantified. Legal scholars observe that "[p]ersonal information is an important currency in the new millennium."[42] Indeed, "[t]he monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend." *Id*. "Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information." *Id*.

82. Numerous empirical studies quantify the appropriate value measure for personal data. Generally, the value of personal data is measured as either the consumer's willingness to

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

accept compensation to sell her data or the consumer's willingness to pay to protect her information.

83. Through their false representations and aiding, agreeing with, employing, permitting, or otherwise causing the Third Parties to track users' Private Communications on the Website using third-party cookies, Defendants are unjustly enriching themselves at the cost of consumer privacy and choice, when the consumer could otherwise have the ability to choose if and how they would monetize their data.

PLAINTIFF'S EXPERIENCES

84. On or around March 2023, Plaintiff visited the Website to browse information about Burger King products and locations.

85. When Plaintiff visited the Website, the Website immediately presented him with Defendants' popup cookie consent banner, which provided the option to accept cookies or choose the manage "Cookie Settings" button. Plaintiff viewed Defendants' representation on the popup cookie consent banner that, "This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising, and analytics partners."

86. Consistent with his typical practice in rejecting or otherwise declining the placement or use of cookies and tracking technologies, Plaintiff clicked the manage "Cookie Settings" button. The Website then displayed to Plaintiff the cookie consent preferences window. Plaintiff moved the toggle to the left to opt out of the sale/sharing of his personal information and opt out of all cookies, except those that were strictly necessary, including targeting cookies and performance cookies, and clicked the "Confirm My Choices" button. Plaintiff believed that toggling off the "Sell or Share My Personal Information" option would allow him to opt out of, decline, and/or reject all non-required cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of user data to third-party social media, advertising, and analytics companies for the purposes of providing personalized content, advertising, and analytics services).

87. In toggling off the "Sell or Share My Personal Information" option, Plaintiff gave Defendants notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Website. Further, Plaintiff specifically rejected, based on Defendants' representations, those cookies cause the disclosure of user data to third-party social media, advertising, and analytics companies for the purposes of providing personalized content, advertising, and analytics services. In reliance on these representations and promises, only then did Plaintiff continue browsing the Website.

88. Even before the popup cookie consent banner appeared on the screen, Defendants nonetheless caused cookies and tracking technologies, including those that cause the disclosure of user data to third-party social media, advertising, and analytics companies, to be placed on Plaintiff's device and/or transmitted to the Third Parties along with user data, without Plaintiff's knowledge. Accordingly, the cookie consent preferences window's representation to Plaintiff that he could opt out of the sale/sharing of his personal information and opt out of all non-required cookies and tracking technologies while he browsed the Website was false. Contrary to what Defendants made Plaintiff believe, he did not have a choice about whether third-party cookies would be placed on his device and/or transmitted to the Third Parties along with his user data; rather, Defendants had already caused that to happen.

89. Then, as Plaintiff continued to browse the Website in reliance on the promises Defendants made in the cookie consent banner and cookie consent preferences window, and despite Plaintiff's clear rejection of the use and/or placement of such cookies and tracking technologies, Defendants nonetheless continued to cause the placement and/or transmission of cookies along with user data, including those that cause the disclosure of user data to the Third Parties on his device. In doing so, Defendants permitted the Third Parties to track and collect Plaintiff's Private Communications as Plaintiff browsed the Website.

90. Defendants' representations to Website users that they could opt out of the sale/sharing of his personal information and opt out of all cookies were untrue. Had Plaintiff known this fact, he would not have used the Website. Moreover, Plaintiff reviewed the popup

cookie consent banner, cookie consent preferences window, and Privacy Statement prior to using the Website. Had Defendants disclosed that they would continue to sell/share personal information and cause cookies and tracking technologies to be stored on consumers' devices even after they choose to opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies, Plaintiff would have noticed it and would not have used the Website or, at a minimum, he would have interacted with the Website differently.

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

ARBITRATION PROCEEDING AND TOLLING

92. The delayed discovery rule applies to Plaintiff's claims. Plaintiff was unaware that even though he rejected cookies on the Website, Defendants caused cookies, including the

Third Parties' cookies, to be sent to his browser, stored on his devices, and transmitted to the Third Parties along with his private user data until on or around October 20, 2023 when he learned of Defendants' privacy violations from his counsel.

93. On or about November 2023, Plaintiff's counsel notified Defendants that Plaintiff alleged that they knowingly (and without consent) cause third-party cookies and corresponding data to be stored on consumers' devices and/or transmitted to third parties when they visit the Website despite consumers' clear rejection or declination of such third-party cookies.

94. In response, Defendants asserted that Plaintiff's claims were subject to arbitration by virtue of the Website's "Terms of Service," which includes an arbitration agreement and class action waiver. Plaintiff's counsel explained that Plaintiff did not take any action to manifest his assent to the Terms of Service (such as checking a box or clicking a link) and therefore the arbitration provision was inapplicable to Plaintiff's claims. Defendants disagreed and claimed that Plaintiff's dispute was subject to the Terms of Service.

95. Accordingly, on or about November 13, 2023, Plaintiff timely filed an arbitration demand against Defendants with the American Arbitration Association ("AAA"), Case No. 01-23-0005-1398 in which he provided Defendants with notice of the claims asserted in this Complaint and his intent to pursue those claims on behalf of other similarly situated class members.

96. In his arbitration demand, Plaintiff alleged, *inter alia*, that he did not assent to the Website's Terms of Service and the purported arbitration provision was unenforceable against him. Plaintiff indicated his intent to pursue his claims in court should the arbitrator determine that his claims were not subject to arbitration. Plaintiff filed a Motion re Non-Arbitrability in the arbitration proceeding in which he argued that the Website's arbitration provision was not enforceable against him and that he was entitled to pursue these claims in court.

97. The arbitrator issued an order on Plaintiff's Motion re Arbitrability on July 9, 2024 in which he ruled that the court, not the arbitrator, must decide whether an arbitration agreement was formed between the parties. Further the arbitrator concluded that "This case will

be placed on administrative hold, pending a court determination of whether an enforceable arbitration agreement was formed."

98. Despite exercising reasonable diligence, Plaintiff was unaware of Defendants' fraudulent and unlawful conduct alleged herein due to their active concealment of material facts, which prevented Plaintiff from discovering his claims within the statute of limitations. Further, Plaintiff's claims were equitably tolled by the filing of the arbitration proceeding because Defendants had notice of his claims (and his intent to pursue them in court) and asserted that his claims were subject to arbitration. Defendants were not prejudiced in their ability to gather evidence for Plaintiffs' claims since his claims were substantially similar in the arbitration proceeding than those asserted in this Complaint. These extraordinary circumstances, including Defendants' intentional misrepresentations and Plaintiff's pursuit of his claims in the arbitration proceeding, warrant tolling the statute of limitations to allow Plaintiff to pursue his claims in this forum. Plaintiff acted in good faith and engaged in reasonable conduct in filing his Complaint in this action while his claims in the arbitration are placed on administrative hold.

CLASS ALLEGATIONS

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

Class: All persons who browsed the Website in the State of California after opting out of the sale/sharing of their personal information in the cookies consent preferences window.

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

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

102. **Common Questions Predominate:** This action involves common questions of law and fact to the Class because each class member's claim derives from the same unlawful conduct that led them to believe that Defendants would not cause third-party cookies to be placed on their browsers and devices and/or transmitted to third parties along with user data, after Class members chose to opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies on the Website, nor would Defendants permit third parties to track and collect Class members' Private Communications as Class members browsed the Website.

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

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

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

104. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, Plaintiff, like the other Class members, visited the Website, opted out of the sale/sharing of his personal information, and had his confidential Private Communications on the Website intercepted by the Third Parties.

105. **Adequacy of Representation:** Plaintiff will fairly and adequately protect the interests of all Class members because it is in his best interests to prosecute the claims alleged herein to obtain full compensation due to him for the unfair and illegal conduct of which he

complains. Plaintiff also has no interests in conflict with, or antagonistic to, the interests of Class members. Plaintiff has retained highly competent and experienced class action attorneys to represent his interests and those of the Class. By prevailing on his claims, Plaintiff will establish Defendants' liability to all Class members. Plaintiff and his counsel have the necessary financial resources to adequately and vigorously litigate this class action, and Plaintiff and counsel are aware of their fiduciary responsibilities to the Class members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for Class members.

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

CAUSES OF ACTION

First Cause of Action: Invasion of Privacy

107. Plaintiff realleges and incorporates the paragraphs of this Complaint as if set forth herein.

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

109. Defendants have intruded upon the following legally protected privacy interests of Plaintiff 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) Plaintiff's and Class members' Fourth Amendment right to privacy.

110. Plaintiff and Class members had a reasonable expectation of privacy under the circumstances, as Defendants affirmatively promised users they could opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies before proceeding to browse the Website. Plaintiff and other Class members directed their electronic devices to access the Website and, when presented with the popup cookies consent banner on the Website, Plaintiff and Class members opted out of the sale/sharing of their personal information and reasonably expected that his and their opt outs would be honored. That is, he and they reasonably believed that Defendants would not permit the Third Parties to store and send cookies and/or use other such tracking technologies on their devices while they browsed the Website. Plaintiff and Class members also reasonably expected that, if they opted out of the sale/sharing of their personal information and opted out of all non-required cookies and tracking technologies, Defendants would not permit the Third Parties to track and collect Plaintiff's and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, on the Website.

111. 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.

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

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

114. Defendants' intrusion into Plaintiff's privacy was also highly offensive to a reasonable person.

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

preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, without their consent.

116. Plaintiff and Class members have been damaged by Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

117. Plaintiff and Class members seeks appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendants as a result of their intrusions upon Plaintiff's and Class members' privacy.

118. Plaintiff and Class members seek punitive damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' opt outs of the sale/sharing of their personal information and opt outs of all non-required cookies and tracking technologies. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

Second Cause of Action: Intrusion Upon Seclusion

119. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

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

121. By permitting third-party cookies and tracking technologies to be stored on consumers' devices without consent, which caused the Third Parties to track and collect Plaintiff's and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, in violation of Defendants' representations otherwise in the popup cookie consent banner, Defendants intentionally intruded upon the solitude or seclusion

of Website users. Defendants effectively placed the Third Parties in the middle of communications to which they were not invited, welcomed, or authorized.

122. The Third Parties' tracking and collecting of Plaintiff's and Class member's Private Communications on the Website using third-party cookies that Defendants caused to be stored on users' devices—and to be transmitted to Third Parties—was not authorized by Plaintiff and Class members, and, in fact, those Website users specifically chose to opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies and Defendant was aware of such opt outs.

123. Plaintiff and the Class members had an objectively reasonable expectation of privacy surrounding his and their Private Communications on the Website based on Defendants' promise that users could opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies, as well as state criminal and civil laws designed to protect individual privacy.

124. Defendants' intentional intrusion into Plaintiff's and other users' Private Communications would be highly offensive to a reasonable person given that Defendants represented that Website users could opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies when, in fact, Defendants caused such third-party cookies to be stored on consumers' devices and browsers, and to be transmitted to third parties, even when consumers opted out. Indeed, Plaintiff and Class members reasonably expected, based on Defendants' false representations, that when he and they moved the toggle to opt out of the sale/sharing of their personal information, Defendants would not cause such third-party cookies to be stored on his and their devices or permit the Third Parties to obtain their Private Communications on the Website, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

125. Defendants' conduct was intentional and intruded on Plaintiff's and users' Private Communications on the Website.

126. Plaintiff and Class members have been damaged by Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

127. Plaintiff and Class members seeks appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendants as a result of their intrusions upon Plaintiff's and Class members' privacy.

128. Plaintiff and Class members seek punitive damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' opt outs of the sale/sharing of their personal information and opt outs of all non-required cookies and tracking technologies. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

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

129. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

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

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

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

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

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication— the right to control the nature and extent of the firsthand dissemination of his statements.

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

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

> [i] Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;
>
> [ii] Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;
>
> [iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

Cal. Penal Code § 631(a).

134. CIPA § 631(a) also penalizes those who [iv] "aid[], agree[] with, employ[], or conspire[] with any person" who conducts the aforementioned wiretapping, or those who "permit" the wiretapping.

135. Defendants are each a "person" within the meaning of California Penal Code § 631.

136. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL

8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

137. 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, Defendants' deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of "any other manner").

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

139. Under § 631(a), Defendants must show that they had the consent of all parties to a communication.

140. At all relevant times, the Website caused Plaintiff and Class members' browsers to store the Third Parties' cookies and to transmit those cookies alongside Private Communications—including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—to the Third Parties without Plaintiff's and Class members' consent. By configuring the Website in

this manner, Defendants willfully aided, agreed with, employed, permitted, or otherwise caused the Third Parties to wiretap Plaintiff and Class members using the Third Parties' cookies and to accomplish the wrongful conduct alleged herein.

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

142. The Private Communications of Plaintiff and Class members, on the one hand, and Defendants, on the other, that the Third Parties automatically intercepted directly communicates the Website user's affirmative decisions, actions, choices, preferences, and activities, which constitute the "contents" of electronic communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

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

144. Plaintiff and Class members did not provide their prior consent to the Third Parties' intentional access, interception, reading, learning, recording, collection, and usage of Plaintiff's and Class members' electronic communications. Nor did Plaintiff and Class members provide their prior consent to Defendants aiding, agreeing with, employing, permitting, or otherwise causing the Third Parties' conduct. To the contrary, Plaintiff and Class members expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic communications by choosing to opt out in the cookie consent preferences window.

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

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

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

148. Unless enjoined, Defendants 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 Plaintiff's and Class members' electronic Private Communications with Defendants. 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 fast food products. Plaintiff, Class members, and the general public continue to desire to use the internet for that purpose. Plaintiff, Class members, and the general public have no practical way to know if his and their request to opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies

will be honored and/or whether Defendants will permit third parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendants. Further, Defendants have already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendants 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)

149. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

150. 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.

151. 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."

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

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

154. At all relevant times, Defendants caused the Third Parties' cookies and the corresponding software code—which are pen registers—to be placed on Plaintiff's and Class

members' browsers and devices, and/or to be used to transmit Plaintiff's and Class members' IP address and user-agent information. *See Greenley v. Kochava,* 2023 WL 4833466, at *15-16 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11 (N.D. Cal. Oct. 21, 2024).

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

156. Plaintiff and Class members did not provide their prior consent to Defendants' use of third-party cookies. On the contrary, Plaintiff and the Class members informed Defendants that they did not consent to the Website's use of third-party cookies by moving the toggle to the left, indicating their choice and/or agreement to opt out of the sale/sharing of their personal information and opt out of all cookies, except those that were strictly necessary, including targeting cookies and performance cookies, and clicked "Confirm My Choices" button.

157. Defendants did not obtain a court order to install or use the third-party cookies to track and collect Plaintiff's and Class member's IP addresses and user-agent information.

158. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members suffered losses and were damaged in an amount to be determined at trial.

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

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

160. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

161. Defendants fraudulently and deceptively informed Plaintiff and Class members that he and they could manage their cookie settings to opt out of the sale/sharing of their personal information and opt out of all non-required cookies.

162. However, despite Defendants' representations otherwise, Defendants 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 clicked manage "Cookie Settings" in the cookie consent banner and moved the toggle to the left in the cookie consent preference window, indicating their choice and/or agreement to opt out of the sale/sharing of their personal information and opt out of all cookies, except those that were strictly necessary, including targeting cookies and performance cookies. These cookies and corresponding software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' Private Communications, even when consumers had previously chosen to opt out of the sale/sharing of their personal information.

163. These misrepresentations and omissions were known exclusively to, and actively concealed by Defendants, not reasonably known to Plaintiff and Class members, and material at the time they were made. Defendants knew, or should have known, how the Website functioned, including the Third Party's resources it installed on the Website and the third-party cookies in use on the Website, through testing the Website, evaluating its performance metrics by means of their accounts with the Third Parties, or otherwise, and knew, or should have known, that the Website's programming allowed the third-party cookies to be placed on users'—including Plaintiff's—browsers and devices and/or transmitted to the Third Parties along with users' Private Communications even after users attempted to opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies, which Defendants promised their users they could do. Defendants' misrepresentations and omissions concerned material facts that were essential to the analysis undertaken by Plaintiff and Class members as to whether to use the Website. In misleading Plaintiff and Class members and not so informing him and them, Defendants breached their duties to Plaintiff and Class members. Defendants also gained financially from, and as a result of, their breach.

164. Plaintiff and Class members relied to their detriment on Defendants' misrepresentations and fraudulent omissions.

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

166. Defendants' actions caused damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their personal information and communications.

167. Defendants' representation that consumers could and opt out of all non-required cookies and tracking technologies (inclusive of those cookies that cause the disclosure of user data to third-party social media, advertising, and analytics companies for the purposes of providing personalized content, advertising, and analytics services) if they moved the toggle in the cookie consent preference window was untrue. Again, had Plaintiff and Class members known these facts, they would not have used the Website. Moreover, Plaintiff and Class members reviewed the popup cookie consent banner, the cookie consent preference window, and the Privacy Statement prior to their interactions with the Website. Had Defendants disclosed that it caused third-party cookies to be stored on Website visitors' devices that cause the disclosure of user data to third-party social media, advertising, and analytics companies and/or share information with third parties even after they choose to opt out all such non-required cookies, Plaintiff and Class members would have noticed it and would not have interacted with the Website.

168. By and through such fraud, deceit, misrepresentations and/or omissions, Defendants intended to induce Plaintiff and Class members to alter their positions to their

detriment. Specifically, Defendants fraudulently and deceptively induced Plaintiff and Class members to, without limitation, use the Website under the mistaken belief that Defendants would not permit third parties to obtain users' Private Communications when consumers chose to reject non-required cookies. As a result, Plaintiff and the Class provided more personal data than they would have otherwise.

169. Plaintiff and Class members justifiably and reasonably relied on Defendants' misrepresentations and omissions, and, accordingly, were damaged by Defendants' conduct.

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

171. Plaintiff and Class members seek punitive damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' rejection of the Website's use of non-required cookies. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

Sixth Cause of Action: Unjust Enrichment

172. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

173. Defendants created and implemented a scheme to increase their own profits through a pervasive pattern of false statements and fraudulent omissions.

174. Defendants were unjustly enriched as a result of their wrongful conduct, including through their misrepresentation that users could opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies and by permitting the Third Parties to store and transmit cookies on Plaintiff's and Class members' devices and browsers, which permitted the Third Parties to track and collect users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs,

session information, user identifiers, and/or geolocation data, even after Class members opted out of such cookies.

175. Plaintiff and Class members' Private Communications have conferred an economic benefit on Defendants.

176. Defendants have been unjustly enriched at the expense of Plaintiff and Class members, and Defendants have unjustly retained the benefits of their unlawful and wrongful conduct.

177. Defendants appreciated, recognized, and chose to accept the monetary benefits that Plaintiff and Class members conferred onto Defendants at his and their detriment. These benefits were the expected result of Defendants acting in their pecuniary interest at the expense of Plaintiff and Class members.

178. It would be unjust for Defendants to retain the value of Plaintiff's and Class members' property and any profits earned thereon.

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

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

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

Eighth Cause of Action: Trespass to Chattels

182. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

183. Defendants, intentionally and without consent or other legal justification, caused cookies to be stored on Plaintiff's and Class members' browsers and devices, which caused the

Third Parties and Defendants to track and collect Plaintiff's and Class members' Private Communications and use the data collected for their own advantage, as described above.

184. Defendants were unjustly enriched as a result of their wrongful conduct, including through their misrepresentation that users could opt out of the sale/sharing of their personal information and opt out of all non-required cookies and tracking technologies, and through their failure to disclose that Defendants cause third-party cookies to be stored on consumers' devices and browsers, which cause the Third Parties and Defendants to track and collect Plaintiff's and Class members' Private Communications even after consumers chose to opt out of such cookies.

185. Defendants intentionally caused third party software code to be stored onto Plaintiff's and Class members' devices, knowing that the code would be executed by those devices. The software code then placed and/or transmitted cookies along with Plaintiff's and Class members' Private Communications to the Third Parties. These intentional acts interfered with Plaintiff's and Class members' use of the following personal property owned, leased, or controlled by Plaintiff and other users: (a) her and their computers and other electronic devices; and (b) her and their personally identifiable information.

186. Defendants' trespass of Plaintiff's and other users' computing devices resulted in harm to Plaintiff and other users and caused Plaintiff and other users the following damages:

a. Nominal damages for trespass;

b. Reduction of storage, disk space, and performance of Plaintiff's and other users' computing devices; and

c. Loss of value of Plaintiff's and other users' computing devices.

PRAYER FOR RELIEF

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

A. A declaration that Plaintiff is not subject to Defendant's Terms of Service;

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

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

D. An award of punitive damages;

E. An award of nominal damages;

F. An order for full restitution;

G. An order requiring Defendants to disgorge revenues and profits wrongfully obtained;

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

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

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

Dated: April 25, 2025