

Victor J. Sandoval, SBN 344461
ALMEIDA LAW GROUP LLC
3415 S. Sepulveda Blvd. Suite 1121
Los Angeles, California 90034
562-534-5907
victor@almeidalawgroup.com

Counsel for Plaintiff & Proposed Classes

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

AMANDA REIMER, *on behalf of
herself and all others similarly
situated,*

Plaintiff,

vs.

BABYCENTER, LLC, EVERYDAY
HEALTH, INC., and ZIFF DAVIS,
INC.

Defendants.

Case No. 2:26-cv-10783

CLASS ACTION COMPLAINT

1. INVASION OF PRIVACY
 2. INTRUSION UPON SECLUSION
 3. VIOLATION OF THE
CALIFORNIA INVASION OF
PRIVACY ACT, CAL. PENAL
CODE § 631
 4. VIOLATION OF THE
CALIFORNIA INVASION OF
PRIVACY ACT, CAL. PENAL
CODE § 632
 5. VIOLATION OF THE FEDERAL
WIRETAP ACT, 18 U.S.C. § 2510,
ET SEQ.
 6. VIOLATION OF THE
CALIFORNIA COMPREHENSIVE
COMPUTER DATA ACCESS AND
FRAUD ACT, CAL. PENAL CODE
§ 502
 7. FRAUD, DECEIT, AND/OR
MISREPRESENTATION
 8. UNJUST ENRICHMENT
 9. BREACH OF CONTRACT
 10. NEGLIGENT
MISREPRESENTATION
 11. INTENTIONAL
MISREPRESENTATION
- DEMAND FOR JURY TRIAL**

1 Plaintiff Amanda Reimer (“Plaintiff”), individually and on behalf of all others
2 similarly situated, brings this class action lawsuit against defendants BabyCenter,
3 LLC (“BabyCenter” or “Defendant”) Everyday Health, Inc. (“Everyday”) and Ziff
4 Davis, Inc. (“Ziff;” together with BabyCenter and Everyday, the “Defendants”) and
5 alleges, upon personal knowledge as to her own actions and her counsel’s
6 investigation and upon information and good faith belief as to all other matters, as
7 follows:

8 INTRODUCTION

9
10 1. Defendants operate the BabyCenter pregnancy and parenting media
11 property, www.babycenter.com (collectively, the “Website”). Through the Website,
12 Defendants publish articles, videos, and interactive tools directed at expectant and
13 new parents, and invites users to create accounts and log detailed personal
14 information about themselves, their pregnancies, and their children. The information
15 Defendants invite users to supply and to generate through their browsing is among
16 the most sensitive that exists: whether a user is trying to conceive, her due date, the
17 week of her pregnancy, the age and development of her child, and the health topics
18 she is researching. Defendants nonetheless caused that information to be disclosed to
19 advertising and analytics companies after its users expressly told Defendants not to.

20 2. The Website incorporates resources and programming scripts from third
21 parties—including Google LLC (through Google Analytics, Google Ad Manager,
22 and DoubleClick) and LiveRamp Holdings, Inc. (through the rlcdn.com and
23 pippio.com identity-resolution services), and the additional entities identified below
24 (collectively, the “Third Parties”)—that use cookies and similar tracking
25 technologies on users who visit the Website. These cookies and tracking technologies
26 transmit data to third parties.

27 3. The Third Parties receiving transmissions from the Website after a user
28 selected “Do Not Consent” include, without limitation: Google LLC

(googlesyndication.com, googleadservices.com, doubleclick.net, google-analytics.com, googletagservices.com, 2mdn.net, gstatic.com, adtrafficquality.google, imasdk.googleapis.com, ampproject.org); LiveRamp Holdings, Inc. (rlcdn.com, pippio.com); Microsoft Corporation (bat.bing.com, bat.bing.net, adnxs.com); Amazon.com, Inc. (amazon-adsystem.com); The Trade Desk, Inc. (adsrvr.org); Magnite, Inc. (rubiconproject.com); Index Exchange, Inc. (casalemedia.com); TripleLift, Inc. (3lift.com); OpenX Technologies, Inc. (openx.net); Comscore, Inc. (scorecardresearch.com); Yahoo Inc. (analytics.yahoo.com); IPONWEB GmbH (bidswitch.net); DoubleVerify Inc. (doubleverify.com, dv.tech); Integral Ad Science, Inc. (adsafeprotected.com); Kargo Global, Inc. (kargo.com); RTB House S.A. (creativecdn.com); ID5 Technology Ltd. (id5-sync.com); Tapad, Inc. (tapad.com); Neustar, Inc. (agkn.com); Criteo S.A. (media6degrees.com); Outbrain Inc. (outbrain.com); StackAdapt Inc. (stackadapt.com); Adobe Inc. (everesttech.net); Eyeota Pte. Ltd. (eyeota.net); 33Across, Inc. (33across.com); Opera Limited (adx.opera.com, oa.opera.com); Blis Media Limited (blismedia.com); Beeswax (bidr.io); iPredictive (ipredictive.com); Sitescout (sitescout.com); Amobee/Turn (turn.com); Upwave/Survata (survata.com); JW Player (jwplayer.com, jwpltx.com); Ozone Project Limited (the-ozone-project.com); Adlightning (adlightning.com); and Whaleco Inc. d/b/a Temu (temu.com).

4. This Complaint describes the collection performed by Google and LiveRamp in detail, and uses them to illustrate the conduct at issue. The illustration is not a limitation. Each of the Third Parties identified above received transmissions from Plaintiff's and Class members' browsers after those users refused consent; each is a separate legal entity that is not a party to the communications between the user and Defendant; and each had and exercised the capability to use what it received for its own commercial purposes.

1 5. Defendants did not deploy these technologies by accident or by default.
2 Defendants administer the Website’s cookie consent banner through a consent-
3 management platform, which permits the operator to specify, for each category of
4 cookie and for each jurisdiction, whether a given tag may fire before consent, after
5 consent, and after a refusal of consent. Those settings are configured and maintained
6 by the website operator—here, Defendant—and not by the Third Parties. Defendants
7 therefore controlled, at all relevant times, whether its users’ refusals would be
8 honored.

9 6. The Website offers users the option to choose between “I Consent” and
10 “Do Not Consent” to cookies, the latter allowing users to avoid tracking by
11 advertisers and data brokers.

12 7. Defendants’ Privacy Policy separately represents that Defendants
13 respect users’ privacy and that users may control the use of cookies and similar
14 technologies on the Website.

15 8. Users who select “Do Not Consent” to cookies reasonably expect that
16 the Website will not place or cause to be placed any cookies, particularly those used
17 for advertising, analytics, or cross site tracking. The same goes for users who reject
18 only some and not all cookies. Those users expect that the Website will not place or
19 cause to be placed any cookies that they have rejected. But even for those users who
20 have rejected cookies (whether some or all), the Website continues to enable the
21 Third Parties to place or transmit advertising, analytics, and/or tracking cookies.
22 These cookies and their associated network requests capture private communications
23 and interactions between users and Defendant, including health information such as
24 pregnancy due dates.

25 9. Website users, including Plaintiff, reasonably expected that their
26 communications with Defendants would remain confidential between themselves
27 and Defendants. California law prohibits the recording or eavesdropping upon
28

1 confidential communications without consent. Cal. Penal Code § 632. The California
2 Supreme Court has held that a “confidential communication” under § 632 takes place
3 “if a party to the conversation has an objectively reasonable expectation that the
4 conversation is not being overheard or recorded.” *Flanagan v. Flanagan*, 27 Cal. 4th
5 766, 41 P.3d 575 (2002). Health-related communications give rise to a reasonable
6 expectation of confidentiality. *See Yockey v. Salesforce, Inc.*, 688 F. Supp. 3d 962
7 (N.D. Cal. 2023); *Doe v. GoodRx Holdings, Inc.*, 2025 WL 2052302 (N.D. Cal. Jul.
8 25, 2025); *M.G. v. Therapymatch, Inc.*, 2024 WL 4219992 (N.D. Cal. Sept. 16, 2024).
9 That expectation was heightened here: the Website invites users to disclose
10 pregnancy status, due dates, fertility and health information, and details about their
11 children, and users reasonably understood that such sensitive family and health
12 information would not be routed to advertising and analytics companies—
13 particularly after they rejected cookies. This expectation is further supported by
14 Plaintiff’s explicit indication that she did not consent to the sharing of her information
15 when she selected “Do Not Consent” on the Website’s cookie banner.

16 10. Worse still, the tracking did not wait for the user to choose. Defendants
17 caused third-party cookies to be placed and third-party network requests to be
18 transmitted before the cookie consent banner was displayed and before the user had
19 any opportunity to accept or refuse. By the time Defendants asked Plaintiff and Class
20 members for permission, Defendants had already taken what it was purporting to ask
21 for.

22 11. The Third Parties use the data they collect from users to analyze and
23 track behavior across different websites and over time. They use this information to
24 build and monetize detailed consumer profiles that include users’ interests,
25 preferences, and demographic characteristics. These profiles are used to group
26 individuals into audience segments—such as “expectant parents,” “new mothers,” or
27 “baby product shoppers”—for targeted advertising and marketing analysis.
28

1 a publicly traded digital media company and is the ultimate parent of BabyCenter,
2 LLC.

3 19. Defendant Everyday Health, Inc. is a Delaware corporation with its
4 principal place of business at 360 Park Avenue S, New York, New York 10010.
5 Everyday Health, Inc. is a wholly owned subsidiary of Ziff Davis, Inc. BabyCenter,
6 LLC operates within the Everyday Health Group Pregnancy & Parenting division.

7 20. Each Defendant owned, operated, controlled, or participated in the
8 operation of the Website during the Class Period. The consent-management platform
9 that governs whether third-party tags fire on the Website after a user refuses consent
10 is administered at the enterprise level across Defendants' pregnancy, parenting, and
11 health properties, and the rule sets, tag-firing conditions, and consent categories
12 applicable to the Website were configured, approved, and maintained by Defendants
13 jointly rather than by BabyCenter alone.

14 21. The Privacy Policy and the consent banner displayed on the Website
15 was drafted, approved, and promulgated by Ziff Davis, Inc. and/or Everyday Health,
16 Inc. for use across their digital properties. Indeed, it specifically names "Everyday
17 Health, Inc., with its parents" as owning and operating the Website. The
18 representations quoted in this Complaint are therefore the representations of each
19 defendant.

20 22. Each Defendant acted as the agent, servant, partner, or joint venturer of
21 each other defendant, and in concert with them, with respect to the conduct alleged.
22 Each defendant ratified and adopted the acts of the others. Plaintiff alleges in the
23 alternative that if any Defendant did not itself own, operate, or control the Website,
24 it directed, authorized, or knowingly aided and abetted the conduct of the Defendants
25 that did.

26 //

JURISDICTION AND VENUE

23. This Court has original subject matter jurisdiction over Plaintiff's claim under the Federal Wiretap Act, 18 U.S.C. § 2510, et seq., pursuant to 28 U.S.C. § 1331, and supplemental jurisdiction over Plaintiff's state-law claims pursuant to 28 U.S.C. § 1367(a) because those claims arise from the same case or controversy.

24. The exercise of federal subject matter jurisdiction is independently appropriate pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) ("CAFA"), because (i) at least one member of the Class is a citizen of a different state than any defendant, (ii) there are more than 100 members of the Class, (iii) the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and (iv) none of the exceptions apply to this action.

25. This Court has personal jurisdiction over each defendant because they conduct business in this judicial district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the judicial district.

26. Venue is proper pursuant to 28 U.S.C. § 1391(b)(1) and 28 U.S.C. § 1391(d) because Defendants would be subject to personal jurisdiction in this District if this District were a separate state, given that Defendants operated and made the Website available to consumers in this District, including Plaintiff. Venue is also proper under 28 U.S.C. § 1391(b)(2) because a substantial part of Defendants' conduct giving rise to the claims occurred in this District, including Plaintiff's use of the Website from her residence in Ventura County.

FACTUAL ALLEGATIONS

I. WEBSITES AND COOKIES

27. Every time someone visits a website, their browser communicates with the website's server using HTTP requests—typically "GET" or "POST" requests. For example, when a user clicks a link, their browser sends a GET request to the website's server asking for a specific page. The server then responds with the content

1 of that page. These requests include the user's Internet Protocol (IP) address so the
2 server knows where to send the response.

3 28. An IP address is a unique numerical label assigned to each device
4 connected to the internet. It serves two principal functions: identifying the host or
5 network interface and providing the location of the device within the network. IP
6 addresses are typically expressed in IPv4 format as four sets of numbers separated
7 by periods (e.g., 192.168.0.1). When a user connects to a website, their browser
8 includes the device's IP address in each request so the server knows where to send
9 the response. Because IP addresses can often be linked to a geographic location or
10 Internet Service Provider, they can be used to identify a user's city, region, or
11 location.

12 29. The Website integrates third-party resources into its website code—
13 software components or content delivered by outside entities such as advertising
14 networks, analytics providers, and social media platforms. These third-party
15 resources are embedded through programming scripts, image tags, pixels, or iframes,
16 and are typically loaded directly from external servers not operated by the Website.
17 These third-party resources include tracking and advertising scripts, analytics
18 libraries, tracking pixels, and social media plug-ins. When a user visits the Website,
19 these embedded elements cause the user's browser to automatically send requests to
20 the third-party domains, which in turn may place tracking cookies on the user's
21 device, load tracking pixels, or execute scripts that monitor user behavior. The use of
22 such third-party technologies is governed by separate agreements between
23 Defendants and the third-party vendor, and enables the vendor to collect data for
24 behavioral advertising, analytics, and user profiling purposes.

25 30. When users visit the Website, their browsers are instructed to send and
26 receive cookies—small text files that store data associated with the user's device and
27 browsing session. Each time a user navigates to a new page within the Website or
28

1 returns to the Website in a new session, the browser makes network requests to the
2 Website's servers, and third-party servers, to load the page and its associated
3 resources (HTML, CSS, JavaScript, images, trackers, etc.). These cookies are
4 automatically included with the network requests to the Website and its third-party
5 partners, allowing them to identify the user and remember prior activity.

6 31. Cookies generally contain a unique identifier that enables persistent
7 tracking over time. By reading this identifier, the receiving server can distinguish one
8 user from another and maintain a continuous session profile, even across multiple
9 visits. In addition to identifiers, cookies can store other data, such as user preferences,
10 login tokens, language settings, and tracking parameters that link behavior across
11 different sites and platforms. When embedded third-party resources (such as ad
12 scripts or analytics tags) load on the Website, they can cause the user's browser to
13 transmit or receive third-party cookies—cookies set by a domain other than the
14 Website itself. These third-party cookies can be used to create behavioral profiles,
15 monitor advertising effectiveness, and retarget users with personalized ads based on
16 their browsing history.

17 32. First-party cookies are those set directly by the Website's own domain.
18 When a user interacts with the Website—for example, by browsing listings, running
19 searches, or navigating between internal pages—the Website may store identifying
20 information in cookies created under its own domain name (e.g., babycenter.com).
21 These cookies are used to maintain user session data, remember preferences, and
22 record repeat visits. Because the cookies are tied to the Website's domain, they are
23 automatically sent back to the Website with each HTTP request the user makes while
24 navigating within the site.

25 33. Third-party cookies are set by domains other than the Website's own.
26 When the Website loads embedded resources—such as advertising scripts, analytics
27 tools, or social media widgets—those third-party elements can instruct the user's
28

1 browser to send or receive cookies associated with the third party's domain (e.g.,
2 doubleclick.net, google-analytics.com, id.rlcdn.com). The browser includes these
3 cookies when sending requests to those external domains, allowing the third party to
4 recognize returning users across different websites. Third-party cookies typically
5 contain a persistent identifier, enabling the third party to track the same user across
6 multiple browsing sessions and unrelated websites. This cross-site tracking allows
7 the third party to build a profile of the user's online behavior, preferences, and
8 demographics.

9 34. Cookies are often linked to network requests—data (including the
10 cookie) sent from the user's browser to a third party server—which allows third
11 parties to track user behavior across websites and over time.

12 35. Third-party cookies enable third parties to track in real time and collect
13 Website users' personal information such as browsing activities and Private
14 Communications with Defendant, including the following (collectively, the "Private
15 Communications"):

- 16 a. Browsing history: Records of the pages a user visits on the
17 website, the order in which those pages are accessed, how the user
18 navigates between them, and whether the user is returning or
19 visiting for the first time. This data allows the tracker to
20 reconstruct a full map of the user's interaction with the site.
- 21 b. Visit history: Information about how often and when a user
22 returns to the Website— including visit counts, dates, times, and
23 span between visits—enabling the creation of a usage timeline
24 that shows frequency and patterns over time.
- 25 c. Website interactions: Clicks, form actions, scrolls, and other
26 interactive components. This data reveals what users are
27 interested in or intending to do and is used for conversion
28

1 tracking, user intent modeling, and interface optimization User
2 input data: Websites often include interactive features—such as
3 search bars, dropdown filters, zip code locators, or form fields—
4 that allow users to enter information manually.

5 d. Demographic information: Inferred over time from user behavior,
6 device characteristics, and external datasets. Users are placed into
7 audience segments based on likely age, gender, income, lifestyle,
8 family status, or shopping intent (e.g., “expectant parents” or
9 “first-time mothers”).

10 e. Interests and preferences: Information about a user’s preferred
11 content categories or topics—like fertility, pregnancy stages,
12 infant health, or baby products—is captured from repeated visits
13 to relevant pages or engagement with specific types of listings.
14 This data supports interest-based advertising and
15 recommendation engines.

16 f. Shopping behavior: In addition to explicit inputs, trackers collect
17 data about how users interact with the site’s content and listings.
18 This includes products or listings the user viewed, items the user
19 saved, favorited, or added to comparison lists, pages the user
20 revisited or browsed multiple times, time spent on specific
21 listings, and navigation paths that indicate decision-making. This
22 behavioral data allows third parties to model a user’s stage in the
23 purchasing funnel, infer their preferences and price sensitivity,
24 and tailor future ad delivery accordingly—including across
25 unrelated websites and apps.
26
27
28

- g. Device information: Details about the type of device (mobile, desktop, tablet), OS (e.g., iOS, Android), and browser/version (e.g., Chrome 124).
- h. Referring URL: The referrer reveals the previous webpage visited before landing on the current page. This may include internal navigation data or external sources (e.g., search engines) and query parameters disclosing user search behavior.
- i. Session information: Session start/end timestamps and duration data. A key metric for profiling user engagement and determining how long a user is exposed to specific content or ads.
- j. User identifiers: Persistent cookie or ID values used to link activity across sessions/sites.
- k. Geolocation data: Location information based on the Website user's IP address or GPS data, if accessible.
- l. IP address: The user's IP address is sent with most HTTP requests and can be used to infer location (city or ZIP code), identify internet service provider, and detect network type (e.g., mobile, corporate, residential).

36. Third-party cookies are used for a variety of purposes, including analytics (tracking and analyzing user behavior, user engagement, and effectiveness of marketing), personalization (remembering a user's browsing history and purchasing preferences to enable product recommendations), advertising/targeting (delivering targeted advertisements based on a user's profile), and social media integration. They also enable retargeting—showing users ads for products they previously viewed—as well as audience segmentation, attribution analysis, and synchronization of user identifiers across multiple adtech platforms. This allows third parties to construct detailed, persistent profiles of individual users based on their

1 online behavior, preferences, and demographic characteristics. The resulting profiles
2 are used to deliver interest-based advertising, conduct real-time bidding, and build
3 audience segments for resale or further monetization.

4 **II. DEFENDANTS' WEBSITE**

5 37. Defendants operate an interactive pregnancy and parenting content and
6 community platform at the Website, and users communicate with Defendants when
7 they browse and interact with the Website—including when they read articles, watch
8 videos, use interactive tools, and enter information about themselves and their
9 children.

10 38. These features include, among others, a Pregnancy Due Date Calculator,
11 an Ovulation Calculator, a Baby Names Finder, a Baby Registry Checklist and
12 Builder, week-by-week pregnancy and baby-development trackers, and BabyCenter
13 Community groups—including “Birth Clubs” organized by expected due-date
14 month—each of which invites users to submit information about their fertility,
15 pregnancies, and children directly to Defendant.

16 39. Defendants chose to install or integrate its Website with resources from
17 the Third Parties that, among other things, use cookies. When consumers visit the
18 Website, both first-party cookies and third-party cookies are placed on their devices
19 and/or transmitted. This is caused by software code that Defendants incorporate into
20 its Website, or that Defendants cause to be loaded. Because Defendants control the
21 software code of the Website, they have complete control over whether first-party
22 and third-party cookies are placed on its users' devices and/or transmitted to the Third
23 Parties.

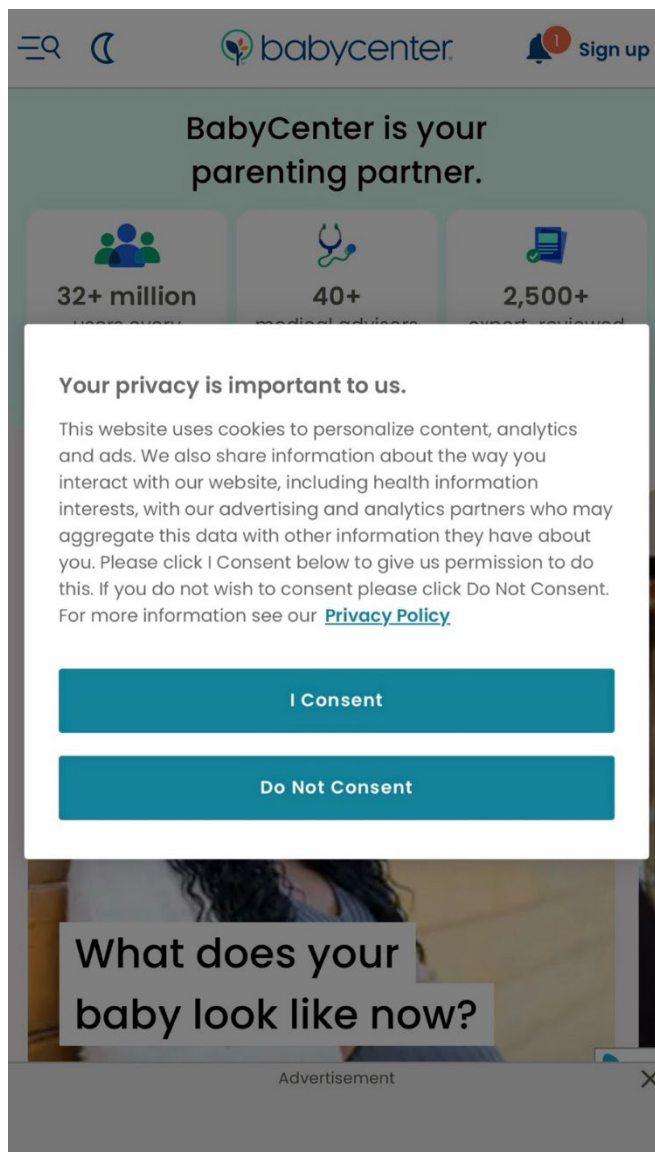
24 //

25 //

26 //

III. DEFENDANTS LIED TO USERS WHEN IT SAID THEY COULD REJECT THE WEBSITE'S USE OF COOKIES.

40. When users in California visited the Website, it immediately displayed to them a popup cookie consent banner titled "Your privacy is important to us." The banner stated in full: "This website uses cookies to personalize content, analytics and ads. We also share information about the way you interact with our website, including health information interests, with our advertising and analytics partners who may aggregate this data with other information they have about you. Please click I Consent below to give us permission to do this. If you do not wish to consent please click Do Not Consent. For more information see our Privacy Policy."



41. Users were given the option to select “I Consent” or “Do Not Consent,” with the Privacy Policy hyperlinked in the banner.

42. The Privacy Policy¹ reinforces the banner’s promise. It states that Defendants may process users’ information on the basis of consent only “where we have obtained your prior, express consent to the Processing,” and that “this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way.” The Privacy Policy also states that Defendants maintain “[c]onsent records,” i.e., “records of any consents you may have given, together with the date and time, means of consent and any related information (e.g., the subject matter of the consent).”

BabyCenter.com Privacy Portal

English

BabyCenter.com is committed to protecting privacy and personal data. To simplify the process of making a request regarding personal data, and to ensure that we respond as rapidly as possible, we’ve created this Privacy Portal.

To make a request regarding personal data, please choose an option below:

Delete My Information

Access My Information

Correct My Information

Opt Out of Sale or Sharing of My
Information

Restrict Processing of My
Information

Objection to Processing of My
Information

Agent Request

Consent Record

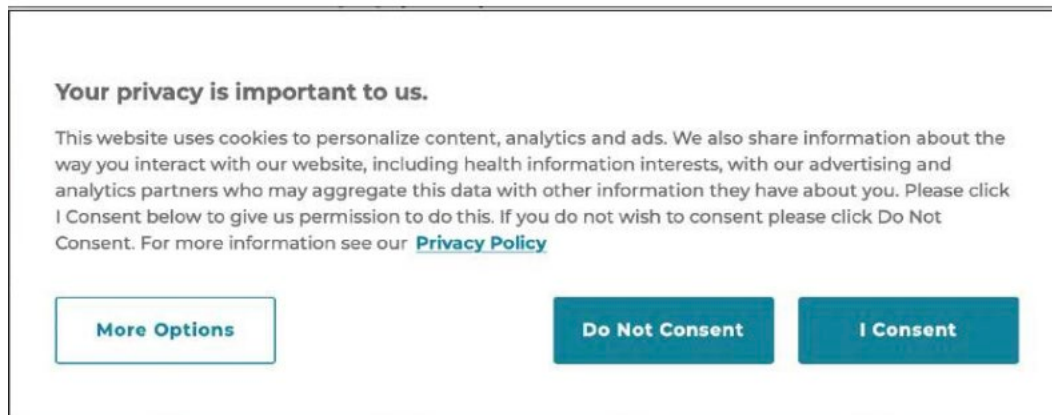
Appeals

43. The Privacy Policy further recognizes users’ “Right to Object to the Use of Sensitive Personal Information,” which it defines to include “information about

¹ BabyCenter, *Privacy Policy*, <https://www.babycenter.com/help-privacy> (last visited Sept. 18, 2026).

1 your health, race, religion, sexual orientation, gender identity, political opinions or
 2 philosophical beliefs.”

3 44. Website users who clicked or elected the “Do Not Consent” button,
 4 indicating their choice and/or agreement to decline all cookies and tracking
 5 technologies in use on the Website, could then continue to browse the Website, and
 6 the popup cookie consent banner disappeared.



15 45. Defendants’ popup cookie consent banner led Plaintiff, and all other
 16 similarly situated reasonable Website users, to believe that they could decline the
 17 Website’s use of cookies and the sharing of “information about the way you interact
 18 with our website, including health information interests, with our advertising and
 19 analytics partners.” The banner further reasonably led Plaintiff and other similarly
 20 situated Website users to believe that if they clicked the “Do Not Consent” button,
 21 then Defendants would not allow the Third Parties to use cookies to access their
 22 Private Communications with the Website, including their browsing history, visit
 23 history, website interactions, user input data, demographic information, interests and
 24 preferences, shopping behaviors, device information, referring URLs, session
 25 information, user identifiers, geolocation data, and IP address.

26 46. Defendants misled users by claiming their cookie rejection choices
 27 would be honored, when in fact Defendants caused the third-party cookies to be
 28

1 placed on Website users' browsers and devices and/or transmitted to the Third
2 Parties, along with user data, even for users who chose to reject cookies.

3 47. Instead, even when users rejected cookies, including by selecting or
4 clicking the "Do Not Consent" button, Defendants continued to cause the Third
5 Parties' cookies to be placed on users' devices and/or transmitted to the Third Parties
6 along with user data, enabling them to collect user data in real time that disclosed
7 Website visitors' Private Communications, including their browsing history, visit
8 history, website interactions, user input data, demographic information, interests and
9 preferences, shopping behaviors, device information, referring URLs, session
10 information, user identifiers, geolocation data, and IP address.

11 48. Thus, even when users tried to protect their privacy by rejecting cookies,
12 Defendants still installed cookies that transmitted Private Communications to the
13 Third Parties, enabling them to track user behavior and communications.

14 49. The behavior of the third-party cookies deployed on the Website can be
15 observed using network inspection tools that record browser communications. These
16 tools allow examination of the outgoing HTTP requests made by the user's browser
17 as it interacts with the Website. The following screenshots and exhibits, collected
18 using such a tool, demonstrate that third-party cookies were transmitted from the
19 user's device to external third-party domains even after the user clicked the "Do Not
20 Consent" button on the Website's cookie consent banner—indicating that data
21 sharing continued despite the user's expressed intent to opt out of tracking.

22
23 *[Remainder of page intentionally left blank]*
24
25
26
27
28

X	Headers	Payload	Preview	Response	Initiator	Timing
▼ Query String Parameters			View source	View URL-encoded		
rcb		11				
frm		0				
apvc		1				
auid		1229573303.1787506463				
dt		Confirm & Pay - BabyCenter Courses				
tid		AW-10997126978				
en		page_view				
dl		https://courses.babycenter.com/users/checkout/auth				
dr		https://courses.babycenter.com/courses/infant-cpr-first-aid-video-course				
scsrc		www.googletagmanager.com				
rnd		944116925.1789422230				
navt		r				
npa		0				
us_privacy		1YNY				
gpp		DBABLA~BVQqAAAAACA.QA				
gpp_sid		7				
_tu		AAG				
gtm		45be69b1v896833944za200zb856657874zd856657874xec				
gcs		G111				
gcd		13v3v3v3v6I1				
dma		0				
tag_exp		115938465~115938468~118897920~118897930~120213116~120385422~120469145~120469153~120912438				
tft		1789422229919				
tfd		1660				
tids		AW-10997126978				
fmt		8				

[Remainder of page intentionally left blank]

▼ Query String Parameters		View source	View URL-encoded
random	1789425771153		
cv	11		
fst	1789425771153		
bg	ffffff		
guid	ON		
async	1		
en	gtag.config		
gtm	45be69b1h1v896833944za200zb856657874zd856657874xec		
gcd	13v3v3v3v6l1		
dma	0		
tag_exp	115938466~115938469~118897920~118897930~120213116~120385423~120469145~120469153~120474864		
u_w	1920		
u_h	1080		
url	https://courses.babycenter.com/users/checkout/auth		
rcb	10		
frm	0		
tiba	Confirm & Pay - BabyCenter Courses		
hn	www.googleadservices.com		
npa	0		
us_privacy	1YNY		
pscdl	noapi		
auid	1229573303.1787506463		
uaa	arm		
uab	64		
uafvl	Not%3DA%3FBrand;99.0.0.0 Google%20Chrome;151.0.7922.170 Chromium;151.0.7922.170		
uamb	0		
uam			
uap	macOS		
uapv	15.4.0		
uaw	0		
gpp	DBABLA~BVQqAAAAACA.QA		
gpp_sid	7		

[Remainder of page intentionally left blank]

Query String Parameters	View source	View URL-encoded
dtstmp	1789422229750	
did	did-0001	
se	e30	
duid	9a8811bf6fc8--01m0qv04ksvdqf2p6xjsaw7ac8	
tna	v2.7.8	
pu	https://courses.babycenter.com/users/checkout/auth	
us_privacy	1YNY	
wpn	lc-bundle	
refr	https://courses.babycenter.com/courses/infant-cpr-first-aid-video-course	
c	PHRpdGxlPkNvbMZpcm0gJmFtcDsgUGF5IC0gQmFieUNlbnRlciBDb3Vyc2VzPC90aXRzZT48aDEgY2xhc3M9InNyLW9ubHkiPgogICAgICAgIEJhYnlDZW50ZXIqQ291cnNlcwogICAgICAgICAgL2gxPg	

50. As displayed in the examples above, the Chrome Developer Tools’ “Network” tab reveals a detailed log of HTTP transmissions between the user’s browser and various third-party domains while interacting with the Website. Even after the user chooses “Do Not Consent” to cookies, the network activity shows that the user’s browser continues to send GET and POST requests to third-party domains like google.com, doubleclick.net, google-analytics.com, id.rlcdn.com and pippio.com (operated by LiveRamp Holdings, Inc.), bat.bing.com (Microsoft), aax.amazon-adsystem.com (Amazon), adsrvr.org (The Trade Desk), and dozens of others. These requests include transmission of cookies and other identifiers, enabling the Third Parties to receive data about the user’s interactions with the site and Private Communications between the user and Defendant. This transmission occurs automatically, even after a user rejected all cookies and tracking technologies by clicking or selecting the “Do Not Consent” button. All of these network calls are made to Third Parties without the user’s knowledge and despite the user’s explicit rejection of all cookies.

51. Defendants’ own instrumentation records the refusal and proves Defendants’ knowledge of it. Within milliseconds of the user selecting “Do Not Consent,” the Website posts a consent receipt to Defendants’ consent-management vendor and transmits to Google a conversion-measurement event expressly named

1 “zdconsent_RejectedAll.” Defendants therefore knew, contemporaneously and in a
2 record of its own making, that the user had rejected all cookies. Defendants told
3 Google that the user had rejected all cookies. And Defendants then allowed scores of
4 third-parties to continue receiving that user’s communications anyway.

5 52. Website users’ Private Communications, including their health data,
6 browsing history, visit history, website interactions, user input data, demographic
7 information, interests and preferences, shopping behaviors, device information,
8 referring URLs, session information, user identifiers, geolocation data, and IP
9 address are surreptitiously obtained by the Third Parties via these cookies.

10 53. The user navigated from the Website’s homepage to pregnancy-related
11 pages, including pregnancy articles, an ovulation calculator, and a due-date calculator
12 result page rendering a pregnancy due date. This establishes a clear inferential
13 profile: a California user researching fertility and pregnancy topics. This profile,
14 along with other information such as precise location, is then transmitted to Third
15 Parties against user consent.

16 54. Users who interact with the Website and reject cookies, including by
17 selecting or clicking the “Do Not Consent” button have chosen to decline the use of
18 cookies and similar technologies for personalized content, advertising, analytics, or
19 the sale or sharing of their personal information with the Third Parties. Despite this
20 rejection, additional data about users’ behavior and communications is transmitted to
21 the Third Parties, along with cookie data. The third-party cookies that Defendants
22 wrongfully permit to be stored on users’ devices and transmitted to Third Parties
23 allow those Third Parties to track and collect detailed information about users’
24 behavior and communications on the Website, including their Private
25 Communications.

26 55. Third-party cookies allow Third Parties to track users’ behavior across
27 websites and over time. This persistent tracking enables them to correlate and
28

1 combine user data with other datasets to build comprehensive profiles that reflect
2 consumers' behaviors, preferences, and demographics—including purchase intent,
3 online behaviors, and interest categories. These profiles are monetized by Third
4 Parties for advertising, sales, and marketing purposes. Advertisers use them to gain
5 granular insights into users' behavioral characteristics and to deliver targeted
6 advertisements tailored to users' profiles and audience segments.

7 56. The Third Party code that the Website causes to be loaded and executed
8 by the user's browser becomes a wiretap because it allows the Third Parties—entities
9 that are separate and distinct from the parties to the conversation (the user and the
10 Defendant)—to intercept, access, and analyze communications between the user and
11 the Website in real time. When executed, the Third Party code initiates outbound
12 transmissions to the Third Parties' servers, capturing detailed information about the
13 user's interactions with the Website, including page views, clicks, search queries,
14 form inputs, and other behavioral and contextual data. This interception occurs
15 without the user's knowledge or consent. Unlike a tool controlled by a party to the
16 communication, the third-party code operates autonomously on behalf of outside
17 entities who are not participants in the communication. These Third Parties are not
18 mere passive recipients of data; they retain, process, and repurpose the intercepted
19 communications for their own commercial benefit—such as behavioral profiling,
20 targeted advertising, data monetization, and cross-site tracking as described in more
21 detail below.

22 57. The Website includes a search bar and other input fields through which
23 users type information they intend to communicate to Defendants alone. When a user
24 submits a search query, the Website loads a results page whose URL contains the
25 query string itself. The Website then causes that full URL to be transmitted to the
26 Third Parties in the Referer header of outbound network requests, together with
27
28

1 cookies and identifiers. The Third Parties therefore receive the exact words the user
2 typed.

3 58. The same is true of the Website's interactive tools. When a user
4 completes the Pregnancy Due Date Calculator or the Ovulation Calculator, the
5 resulting page URL and the cust_params values transmitted with the ad request
6 encode the substance of what the user told Defendant: her pregnancy stage, her due
7 date, and her child's age.

8 59. The Third Parties do not merely receive and store user data. They
9 operate real-time data-ingestion systems that read, parse, and act upon incoming data
10 as it arrives over the network and before it is written to storage. Those systems must
11 do so in order to function at all: the raw payload transmitted from a user's browser is
12 unusable until it is read.

13 60. At the ingest stage, and before any data is committed to storage, the
14 Third Parties: (i) read or learn or attempt to read or learn and transform the payload
15 into a processable format; (ii) read or learn or attempt to read or learn the identifiers
16 within it to deduplicate events that arrive over both the browser channel and a parallel
17 server-to-server channel; (iii) read or learn or attempt to read or learn and analyze the
18 payload to validate it and screen out invalid or anomalous traffic; and (iv) read or
19 learn or attempt to read or learn and perform real-time analytics on the payload to
20 associate it with a particular user or device and to determine what action—such as
21 serving or bidding on an advertisement—should be taken in response.

22 61. Each of those steps requires contemporaneous access to and reading or
23 learning or attempting to read or learn the contents of the communication while it is
24 in transmission. The Third Parties accomplish them using stream-processing
25 platforms purpose-built to operate on data in motion. Google, for example, developed
26 and operates such systems internally and sells the capability to others as Google
27
28

1 Cloud Dataflow, which Google describes as suitable for real-time streaming analytics
2 and real-time machine-learning analysis of streaming data.

3 62. The Third Parties are therefore are active interceptors that read the
4 contents of Plaintiff's and Class members' communications with Defendants while
5 those communications are in transit.

6 **IV. DEFENDANT'S CONDUCT VIOLATED ITS PROMISES.**

7 63. Defendants' aiding, agreeing with, or otherwise enabling the Third
8 Parties to track users' Private Communications on the Website using third-party
9 cookies—even after users rejected cookies, including by selecting or clicking the “Do
10 Not Consent” button—violates the written assurances it made to users.

11 64. Defendants told users they could choose not to consent to its use of
12 cookies and to the sharing of information about the way they interact with the
13 Website—including health information interests—with its advertising and analytics
14 partners. Even after users chose to reject cookies (including by selecting “Do Not
15 Consent”), the Website disregarded those assurances by deploying the very tracking
16 technologies it promised users they could reject—allowing Third Parties to continue
17 collecting data and Private Communications from users' interactions on the Website.

18 65. Defendants also told users on its cookie consent banner that “[y]our
19 privacy is important to us,” and that it “respects your privacy and the information that
20 you have entrusted to us.” But it does not respect its users' privacy choices and allows
21 the Third Parties to obtain, use, and monetize its users' information even after the
22 users have expressly told Defendants that they reject some or all cookies and don't
23 want their information disseminated.

24 **V. THE WEBSITE COLLECTED CONFIDENTIAL**
25 **COMMUNICATIONS BY USING THIRD PARTY COOKIES.**

26 66. Defendants cause third party cookies to be transmitted to and from
27 Website users' browsers and devices, even after users reject cookies (including
28 advertising and analytics cookies) to and from the doubleclick.net and google.com

domains. Each of these domains is associated with Google LLC's digital advertising and analytics platform that collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.² Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Over 16% of web traffic is tracked by Google's DoubleClick cookies.³ 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.⁴ 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

67. Defendants also cause third-party cookies and network requests to be transmitted to and from domains operated by LiveRamp Holdings, Inc., including id.rlcdn.com, check.analytics.rlcdn.com, and pippio.com. LiveRamp provides identity-resolution services: it assigns and synchronizes persistent identifiers that allow a user to be recognized across websites, devices, and email, and it links those identifiers to hashed email addresses so that a browsing session on one site can be matched to a known individual elsewhere. LiveRamp set the pxrc and rlas3 cookies

² <https://business.safety.google/adscookies/> (last visited Sept. 18, 2026) (Cookies "may be set from a few different domains, including google.com, doubleclick.net, googlesyndication.com, or googleadservices.com, or the domain of our partners' sites").

³ <https://www.ghostery.com/whotracksme/trackers/doubleclick> (last visited Sept. 18, 2026).

⁴ <https://developers.google.com/google-ads/api/docs/conversions/overview> (last visited Sept. 18, 2026) ("Conversion tracking provides key insights into users' actions after viewing or clicking an ad. You can keep track of users who call, buy a product, install a mobile app, and more."); see the Advertising, Analytics, and Personalization sections at <https://policies.google.com/technologies/cookies?hl=en-US> (last visited Sept. 18, 2026).

⁵ <https://policies.google.com/technologies/ads?hl=en-US> (last visited Sept. 18, 2026) ("[W]e may use cookies for a number of purposes, such as . . . to show ads that are likely to be more relevant").

1 on the user's device after the user selected "Do Not Consent." The effect of
2 LiveRamp's presence on the Website is that a user's pregnancy- and parenting-
3 related browsing can be tied not merely to an anonymous cookie but to a person.

4 68. In addition to the APC cookie described below, the
5 securepubads.g.doubleclick.net domain set the IDE cookie on the user's device after
6 the user selected "Do Not Consent." The IDE cookie is set on the .doubleclick.net
7 domain, carries a two-year expiration, and is marked "Secure," "HttpOnly," and
8 "SameSite=none." Because it is scoped to the .doubleclick.net domain and is not
9 partitioned to any single website, the IDE cookie accompanies the user's browser to
10 every other website in Google's advertising network, permitting Google to recognize
11 the same user across unrelated sites and over time.

12 69. Defendants do not merely permit Google to observe its users.
13 Defendants affirmatively supplies Google with an identifier of Defendants' own
14 creation. Each ad request the Website causes to be sent to
15 securepubads.g.doubleclick.net carries a "ppid"—publisher-provided identifier—
16 parameter containing a persistent alphanumeric value assigned to the user by
17 Defendants. The same value is transmitted twice more within the cust_params field,
18 as "zdbb" and as "fpid." Because that identifier originates with Defendants rather
19 than with Google, its transmission cannot be explained as the incidental byproduct
20 of loading a third party's tag. Defendants chose to hand Google a key to its own users,
21 and continued to do so after those users refused consent.

22 70. Google sends cookies when a web user visits a webpage that shows ads
23 served through Google Ad Manager or other Google Marketing Platform products,
24 including those associated with DoubleClick.⁶ When a page includes Google
25 Marketing Platform or Google Ad Manager ad tags—even if no ads are displayed—
26 these tags trigger requests to Google's ad servers, which can then set third-party
27

28 ⁶ <https://business.safety.google/adscookies/> (last visited Sept. 18, 2026).

cookies (via doubleclick.net) in the user’s browser. According to Google, “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.”⁷

71. 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.⁸ To measure a website, a business must create a Google Analytics account and add a small piece of JavaScript measurement code to each page on its site.⁹ Then, every time a user visits a webpage, the tracking code will collect information about how that user interacted with the page.¹⁰ 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.”¹¹

72. 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.

//

//

⁷ <https://support.google.com/admanager/answer/2839090> (last visited Sept. 18, 2026).

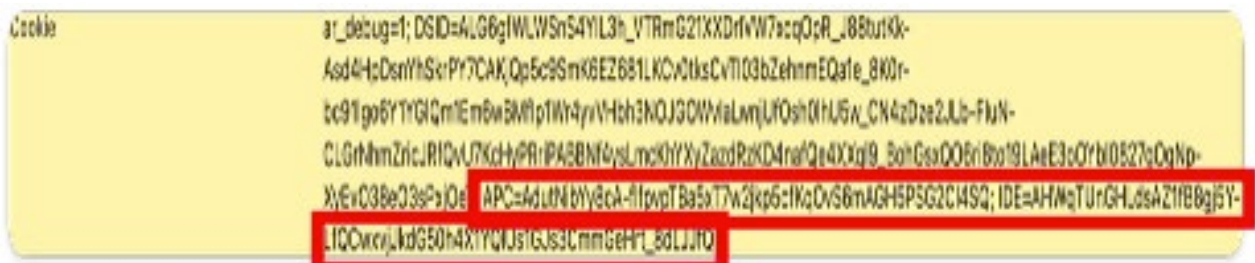
⁸ <https://support.google.com/analytics/answer/12159447> (last visited Sept. 18, 2026).

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Set up events*, <https://developers.google.com/analytics/devguides/collection/ga4/events> (last visited Sept. 18, 2026); and *Recommended events*, <https://developers.google.com/analytics/devguides/collection/ga4/reference/events> (last visited Sept. 18, 2026).

73. For example, even after a user rejects all cookies, the Google software code that Defendants cause to be executed by the Website user's device causes the user's browser to send requests to Google-controlled domains, including securepubads.g.doubleclick.net and googleads.g.doubleclick.net. In response to the request to googleads.g.doubleclick.net—a request directed to Google's Display & Video 360 ad-serving path—Google sets a cookie, the APC cookie, on the user's browser. This cookie acts as a unique identifier and allows Google to recognize the same user across different pages and sessions.



74. The APC cookie is a small data file set by Google's advertising platform, DoubleClick. According to Google, it is an advertising cookie that lasts for 6 months. It is used for these Google products: Campaign Manager, Display & Video 360.

75. The APC cookie contains a unique string of letters and numbers that acts like an ID tag for the user's browser. This ID can be used to recognize a user across different websites that also use Google's ad services. The cookie is set to stay on the user's device for six months unless deleted. It's marked as "Secure," so it's only sent over encrypted (HTTPS) connections. It's also labeled with "SameSite=None," which allows it to be sent even when the user visit websites other than doubleclick.net—this is what makes it a third-party cookie. Finally, it's not marked as "HttpOnly," which means scripts running in a browser (like JavaScript) could potentially access it.

76. The APC cookie is also associated with several network requests. This means that it is associated with specific communications between the browser and Google's servers. These requests are initiated by Third Party code that the Website

1 causes to be loaded and executed by the user's browser, enabling Google to receive
2 data tied to the user's activity on the site.

3 77. In this example, the APC is associated with network requests that
4 transmit Private Communications from the user to Google and Doubleclick. Even
5 after the user rejected all cookies, one particular network request associated with the
6 APC cookie showed Private Communications being communicated to Google as a
7 result of the Website causing the user's browser to execute third party code.

8 78. The user has communicated their content and topic preferences to
9 Defendant, including the pregnancy- and parenting-related content they viewed.
10 They have communicated to the Defendants the specific topics and terms they are
11 looking for. These are all details that the user is communicating to the Defendant.

12 79. These Private Communications are being intercepted by Google and
13 Doubleclick. The browser includes the APC cookie in the request to DoubleClick. Its
14 presence in the request confirms that the browser is sending a persistent user
15 identifier back to Google, allowing DoubleClick to recognize and track the user
16 across sessions and potentially across other websites.

17 80. The network requests associated with the APC cookie contain the
18 following Private Communications:

- 19 a. Browsing history: The url and ref parameters capture the exact
20 web page the user is currently visiting and the page they came
21 from. This allows Google to reconstruct parts of a user's web
22 browsing path. For example, the Website transmits that parameter
23 transmitted to Google the addresses of the pages the user had
24 chosen to read, including a page titled "Am I pregnant?" and its
25 results view, and a page addressing what to expect at a first
26 prenatal appointment. Combined across a session, these values
27 allow Google to reconstruct the user's path through the Website.
28

- 1 b. Visit history: The u_his parameter reports the length of the
2 browser's session history, which informs Google how long or
3 how many pages a user has visited during the current session.
4 That value, combined with the correlator and pvsid session
5 identifiers and the successive url values transmitted during the
6 session, enables Google to reconstruct the user's navigation flow.
- 7 c. Website interactions: Scroll positions (scr_x, scr_y), iframe index
8 (ifi), and timestamps (dt, dlt, idt) reveal how users interact with
9 the page—how far they've scrolled, how long they've stayed, and
10 how quickly they engage with content. This indicates real-time
11 engagement and behavioral responses to ad placements.
12 Additional information is contained in Referring URL and User
13 Input data sections below.
- 14 d. User input data: The cust_params field includes highly specific
15 information about a user's behavior on a pregnancy and parenting
16 site, including content category, pregnancy stage, child age, and
17 article or video topic. These values reflect the user's specific
18 interests and family circumstances and are part of their interaction
19 with babycenter.com.
- 20 e. Interests and preferences: The cust_params field transmits
21 Defendants' own content taxonomy for the page the user is
22 reading, including a content-type value (for example,
23 ct=homepage), a numeric page identifier, and audience-segment
24 lists that Defendants have already assigned to the user.
25 Defendants thereby tell Google not only what the user is viewing
26 but how Defendants has categorized her.
- 27
28

- 1 f. Shopping behaviors: See User input data and Referring URL
2 sections.
- 3 g. Device information: The request includes a set of fields that
4 describe the user's device, such as screen resolution, pixel density,
5 color depth, and time zone offset. These values allow a third party
6 to uniquely identify or “fingerprint” the user’s device.
- 7 h. Page and content identifiers: The network request discloses the
8 full URL the user was viewing on babycenter.com, including the
9 URL path and query parameters identifying the specific content
10 the user chose to view. These choices reflect real-time behavioral
11 preferences, content interests, and family circumstances. When
12 this data is shared with DoubleClick, it allows Google to build a
13 behavioral profile of the user’s pregnancy stage, parental status,
14 and purchasing intent, all without the user directly disclosing that
15 information to Google. By embedding this full URL in a request
16 to DoubleClick, Defendants transmitted the substance of that
17 communication to Google’s ad servers.
- 18 i. Session information: Session-level identifiers like pvsid (page
19 view session ID), correlator, and the session identifiers in
20 cust_params help Google group ad requests within a browsing
21 session and track user flow across pages.
- 22 j. User identifiers: The request transmits parameters like cookie,
23 gpic, user-agent, and uach, all of which transmit user identifiers.
24 The cookie parameter contains a persistent identifier. Its value is
25 unique and is used to track users across sites and over time,
26 supporting ad personalization and frequency capping. The gpic
27 parameter is a user identifier sent to Google. This UID is a unique
28

1 identifier that allows Google to associate the ad request with a
2 particular user profile, even across sessions or websites. It is used
3 for persistent user tracking, audience segmentation, and
4 retargeting, enabling Google to build and refine a behavioral
5 profile based on browsing activity. The request also transmits
6 “user-agent” information to Google: Mozilla/5.0 (Windows NT
7 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
8 Chrome/138.0.0.0 Safari/537.36.13 The user-agent corresponds
9 to the device and browser that the user has used to access the
10 Website. In this case, the user-agent value corresponds to
11 Google’s Chrome browser running on Windows. The uach
12 parameter is a detailed string describing the user agent
13 characteristics. The “user-agent” corresponds to the device and
14 browser that the user has used to access the Website. The value
15 encodes the user's browser (Google Chrome 138), operating
16 system (Windows), and hardware (x86, screen resolution 64).
17 Google uses this to optimize ad rendering and tailor delivery
18 based on device capabilities. This means that even though the user
19 is interacting only with the Website, the data from that interaction
20 becomes part of Google’s cross-site tracking infrastructure. These
21 identifiers are not randomly generated per session—they persist
22 over time and are specifically designed for user recognition.

- 23 k. Geolocation data: The request transmits the user’s IP address,
24 from which city- and ZIP-code-level location is routinely derived,
25 together with a u_tz timezone-offset value. Defendants separately
26 maintain their own geolocation cookies on the user’s device—
27 geoCC, geoCity, geoDMA, geoRegion, and geoZip—reflecting
28

1 that Defendants themselves resolve each visitor to a city, region,
2 designated market area, and postal code.

- 3 1. IP address: Always transmitted in the underlying HTTP request
4 and is always accessible to the receiving server (Google). It is
5 used for geolocation, fraud detection, and ad personalization.

6 81. In response, Google sent back data to the user's browser. That data is
7 contained in a response header. The response header contains fields including
8 google-lineitem-id, google-creative-id, google-mediationgroup-id, and google-
9 mediationtag-id, which Google uses to identify the ad campaign, creative, and
10 mediation configuration responsive to the request. The presence of these fields
11 confirms that the request and the cookies accompanying it are part of Google's ad-
12 targeting and ad-delivery infrastructure, and that the user's browsing behavior was
13 submitted to that infrastructure for evaluation.

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

21 83. Thus, the Google cookies used on the Website enable Google to track
22 users' interactions with advertisements to help advertisers understand how users
23 engage with ads across different websites. Further, the user data collected through
24 the cookie enables the delivery of personalized ads based on user interests and
25 behaviors. For instance, if a user frequently visits travel-related websites, Google will
26 show her more travel-related advertisements. Further, the collected data is used to
27 generate reports for advertisers, helping them assess the performance of their ad
28

1 campaigns and make data-driven decisions (such as renaming their products).
2 Further, Google’s advertising platform enables advertisers to retarget marketing,
3 which Google explains allows advertisers to “show previous visitors ads based on
4 products or services they viewed on your website. With messages tailored to your
5 audience, dynamic remarketing helps you build leads and sales by bringing previous
6 visitors back to your website to complete what they started.”¹²

7 84. Further, in its “Shared Data Under Measurement Controller-Controller
8 Data Protection Terms,” Google states: “Google can access and analyze the Analytics
9 data customers share with us to better understand online behavior and trends, and
10 improve our products and services—for example, to improve Google search results,
11 detect and remove invalid advertising traffic in Google Ads, and test algorithms and
12 build models that power services like Google Analytics Intelligence that apply
13 machine-learning to surface suggestions and insights for customers based on their
14 analytics data and like Google Ads that applies broad models to improve ads
15 personalization and relevance. These capabilities are critical to the value of the
16 products we deliver to customers today.”¹³

17 85. Thus, Google has the capability to use the data it collects for
18 understanding online behavior and trends, machine learning, and improving its own
19 products and services.

20 VI. THE PRIVATE COMMUNICATIONS ARE VALUABLE.

21 86. The Private Communications that the Third Parties track and collect by
22 way of the cookies on the Website are commercially valuable to both Defendants and
23 the Third Parties. Defendants can use the data to measure the performance of its
24 advertising campaigns, assess which articles, videos, and tools are generating
25 interest, and refine its content and user interface accordingly. The behavioral data
26

27 ¹² Dynamic remarketing for web setup guide, <https://support.google.com/google-ads/answer/6077124> (last visited Sept. 18, 2026).

28 ¹³ Shared Data Under Measurement Controller-Controller Data Protection Terms, <https://support.google.com/analytics/answer/9024351> (last visited Sept. 18, 2026).

1 also enables Defendants to segment users based on their preferences and
2 circumstances—such as pregnancy stage, child age, content interests, or product
3 categories—and deliver targeted ads to those users both on and off the Website. The
4 third-party cookies also enable Defendants to target online advertisements to users
5 when they visit other websites, even those completely unrelated to Defendants and
6 its products.

7 87. The Third Parties, including ad platforms like Google, benefit by using
8 the data to create detailed user profiles that persist across browsing sessions and
9 devices. These profiles are used in real-time ad auctions to identify and bid on users
10 who are most likely to convert. For example, if a user browses pregnancy or baby-
11 product content on the Website, that behavior is logged and monetized through
12 higher-value ad placements as that user continues browsing elsewhere. The ability to
13 retarget users across websites, attribute ad performance, and serve tailored content is
14 critical to the digital advertising ecosystem—and it depends on collecting the user’s
15 communications with the Website in real time.

16 88. Data about users’ browsing behavior allows Defendants to identify
17 patterns in how users interact with the Website and what content and products they
18 are interested in—such as specific pregnancy stages, child-development topics,
19 health concerns, or baby-product categories. At a broader level, this information
20 gives Defendants insight into consumer trends across its content and the pregnancy
21 and parenting market as a whole. By collecting and analyzing this data, Defendants
22 are able to refine its marketing strategies, optimize its content and search results, and
23 increase the profitability of the Website.

24 89. The value of Private Communications tracked and collected by the Third
25 Parties using cookies on the Website can be quantified. Empirical studies
26 demonstrate the value of personal data. When tracking is unavailable—i.e., when
27 users can’t be uniquely identified—ad prices drop between 18 % and 23 % on
28

1 average, reducing publisher revenue accordingly.¹⁴ The effect is particularly acute
 2 for publishers like Defendants that offer specialized content. The Network
 3 Advertising Initiative found that behaviorally targeted ads were more than twice as
 4 valuable as non-targeted ads.¹⁵

5 90. 67% of U.S. adults turn off cookies or website tracking to protect their
 6 privacy.¹⁶

7 91. Through its false representations and aiding, agreeing with, or otherwise
 8 enabling the Third Parties to track users' Private Communications on the Website
 9 using third-party cookies, Defendants are unjustly enriching itself at the cost of
 10 consumer privacy and choice, when the consumer could otherwise have the ability to
 11 choose if and how they would monetize their data.

12 **VII. PLAINTIFF.**

13 92. Beginning in or around January 2025 and continuing through in or
 14 around April 2026, Plaintiff Amanda Reimer visited the Website from her home in
 15 Ventura County, California. She used the Website to read articles, watch videos, and
 16 log information about her pregnancy and her infant child, who was then
 17 approximately ten months old. The articles that she read and the videos she watched
 18 concerned issues related to her pregnancy and her infant child. The title of each of
 19 those articles and videos were transmitted to third parties through the URL and
 20 customer event paths discussed above. Similarly, the information she logged was
 21 transmitted through the same.

22
 23
 24 ¹⁴ Rene Laub, Klaus M. Miller & Bernd Skiera, *The Economic Value of User Tracking for Publishers* (Apr. 18, 2024) (unpublished manuscript),
<https://arxiv.org/abs/2303.10906> (last visited Sept. 18, 2026).

25 ¹⁵ See *Study Finds Behaviorally-Targeted Ads More Than Twice as Valuable, Twice as Effective as Non-Targeted Online Ads*, <https://thenai.org/press/study-finds-behaviorally-targeted-ads-more-than-twice-as-valuable-twice-as-effective-as-non-targeted-online-ads/> (May 24, 2010) (last visited Sept. 18, 2026).

27 ¹⁶ Colleen McClain et al., Pew Rsch. Ctr., *How Americans View Data Privacy* (Oct. 18, 2023), <https://www.pewresearch.org/internet/2023/10/18/how-americans-protect-their-online-data/> (last visited Sept. 18, 2026).

1 93. When Plaintiff visited the Website, it immediately presented her with
2 Defendants' popup cookie consent banner, which provided the option to select "I
3 Consent" or "Do Not Consent." Plaintiff viewed Defendants' representation on the
4 popup cookie consent banner that "[t]his website uses cookies to personalize content,
5 analytics and ads" and that Defendants "share information about the way you interact
6 with our website, including health information interests, with our advertising and
7 analytics partners who may aggregate this data with other information they have
8 about you." She also viewed Defendants' representation that if she did not wish to
9 consent she could click the "Do Not Consent" button on the popup.

10 94. Consistent with her typical practice of rejecting or otherwise declining
11 the placement or use of cookies and tracking technologies, Plaintiff selected and
12 clicked the "Do Not Consent" button. Plaintiff believed that selecting the "Do Not
13 Consent" button on the popup cookie consent banner found on the Website would
14 allow her to opt out of, decline, and/or reject all cookies and other tracking
15 technologies (including those that cause the disclosure of user data to third-party
16 social media, advertising, and/or analytics companies for the purposes of providing
17 personalized content, advertising, and analytic services).

18 95. In selecting the "Do Not Consent" button, Plaintiff informed Defendants
19 that she did not consent to the use or placement of cookies and tracking technologies
20 while browsing the Website. Further, Plaintiff specifically rejected, based on
21 Defendants' representations, those cookies that shared her personal information with
22 Defendants' social media, advertising and analytics partners. In reliance on these
23 representations and promises, only then did Plaintiff continue browsing the Website.

24 96. Then, as Plaintiff continued to browse the Website in reliance on the
25 promises Defendants made in the cookie consent banner, and despite Plaintiff's clear
26 rejection of the use and/or placement of such cookies and tracking technologies,
27 Defendants nonetheless continued to cause the placement and/or transmission of
28

1 cookies along with user data, including those involved in providing personalized
2 content, advertising, and analytics services from the Third Parties on her device. In
3 doing so, Defendants permitted the Third Parties to track and collect Plaintiff's
4 Private Communications as she browsed the Website.

5 97. Defendants' representations that consumers could decline consent to
6 cookies by selecting "Do Not Consent" while Plaintiff and users browsed the
7 Website, or at least those involved in providing personalized content, advertising,
8 and analytics services, were untrue. Had Plaintiff known this fact, she would not have
9 used the Website. Moreover, Plaintiff reviewed the popup cookie consent banner and
10 Privacy Policy prior to using the Website. Had Defendants disclosed that it would
11 continue to cause cookies and tracking technologies to be stored on consumers'
12 devices even after they choose to reject all cookies, Plaintiff would have noticed it
13 and would not have used the Website.

14 98. Plaintiff continues to desire to browse content featured on the Website.
15 Plaintiff would like to browse websites that do not misrepresent that users can reject
16 all cookies and tracking technologies. If the Website were programmed to honor
17 users' requests to reject all cookies and tracking technologies, Plaintiff would browse
18 the Website again in the future, but will not do so until then. Plaintiff regularly visits
19 websites that feature content similar to that of the Website. Because Plaintiff does
20 not know how the Website is programmed, which can change over time, and because
21 she does not have the technical knowledge necessary to test whether the Website
22 honors users' requests to reject all cookies and tracking technologies, Plaintiff will
23 be unable to rely on Defendants' representations when browsing the Website in the
24 future absent an injunction that prohibits Defendants from making misrepresentations
25 on the Website. The only way to determine what network traffic is sent to third parties
26 when visiting a website is to use a specialized tool such as Chrome Developer Tools.
27
28

1 As the name suggests, such tools are designed for use by developers. The third parties
2 may also retain Plaintiff's information.

3 **FRAUDULENT CONCEALMENT, DELAYED DISCOVERY, AND**
4 **TOLLING**

5 99. Any applicable limitations period is tolled by the delayed discovery rule.
6 Plaintiff and Class members did not know, and in the exercise of reasonable diligence
7 could not have known, that Defendants continued to cause third-party cookies to be
8 placed on their devices and their communications to be transmitted to the Third
9 Parties after they refused consent. The conduct occurred entirely through automated,
10 non-visible technical processes. Nothing a user could observe on the Website would
11 disclose it. The cookie consent banner vanished after Plaintiff selected "Do Not
12 Consent," which signaled to a reasonable user that her election had been recorded
13 and honored.

14 100. Detecting the conduct requires software-developer tools and the
15 technical training to interpret HTTP network traffic. Plaintiff has neither. Plaintiff
16 did not discover, and could not reasonably have discovered, the facts giving rise to
17 her claims until on or about July 31, 2026, when counsel's investigation of the
18 Website revealed them to her.

19 101. Defendants are further estopped from asserting a limitations defense by
20 its own fraudulent concealment. Defendants affirmatively represented that users
21 could refuse consent, while concealing that the tracking would continue regardless
22 of their election. Defendants' Privacy Policy compounded the concealment by
23 representing that Defendants maintained "[c]onsent records" documenting each
24 user's election. That combination of affirmative misrepresentation and concealment
25 prevented Plaintiff and Class members from discovering their claims and warrants
26 tolling.
27
28

102. Independent of tolling, Defendants’ conduct is a continuing violation. Defendants’ interception, disclosure, and use of Plaintiff’s and Class members’ Private Communications is not a single completed act. It is an ongoing course of conduct that began before this action was filed, continued throughout the limitations period, and continues today. Each time a Class member who has refused consent loads a page of the Website, Defendants cause a fresh set of requests to be transmitted to the Third Parties, a fresh set of cookies to be placed on or read from that member’s device, and a fresh set of Private Communications to be disclosed. Defendants have not ceased the conduct, has not disclosed it, and has not repaired it. Because the unlawful course of conduct extended into the limitations period and persists, Plaintiff’s and Class members’ claims are timely in their entirety.

103. In the alternative, each transmission is a discrete, separately actionable wrong that triggers its own limitations period under the doctrine of continuous accrual. Plaintiff and Class members may therefore recover for every violation occurring within the applicable limitations period preceding the filing of this Complaint and for every violation occurring afterward, without regard to when Defendants’ course of conduct began.

CLASS ALLEGATIONS

104. Plaintiff brings this proposed class action lawsuit pursuant to Federal Rule of Civil Procedure 23(b)(2) and Rule 23(b)(3) on behalf of herself and a Class (the “Class”) and a California subclass (the “California Subclass”; together with the Class, the “Classes”) of all others similarly situated, defined as follows:

- a. **Nationwide Class**: All persons who browsed the Website after rejecting some or all cookies within the applicable statute of limitations (subject to any applicable tolling) (the “Class Period”).

- 1 b. **California Subclass**: All persons who browsed the Website in
2 the State of California after rejecting some or all cookies within
3 the Class Period.

4 105. Excluded from the Classes are: (i) any Judge or Magistrate presiding
5 over this action and members of their families; (ii) Defendant, Defendants'
6 subsidiaries, parents, successors, predecessors, and any entity in which Defendants
7 have a controlling interest and its officers and directors; (iii) persons who properly
8 execute and file a timely request for exclusion from the Class; (iv) persons whose
9 claims in this matter have been finally adjudicated on the merits or otherwise
10 released; (v) Plaintiff's counsel and Defendants' counsel; and (vi) the legal
11 representatives, successors, and assigns of any such excluded persons.

12 106. **Numerosity**: The exact number of members of the Classes is unknown
13 and not available to Plaintiff at this time, but individual joinder is impracticable. On
14 information and belief, Defendants have many thousands of users who fall into the
15 definition of the Classes. Members of the Classes can be identified through
16 Defendants' records.

17 107. **Commonality and Predominance**: There are questions of law and fact
18 common to the claims of Plaintiff and the alleged Classes, and those questions
19 predominate over any questions that may affect individual members of the Classes.
20 Common questions for the members of the Classes include, but are not necessarily
21 limited to the following:

- 22 a. Whether Defendants' Website honored the choices of the users of
23 its Website to reject cookies;
24 b. whether Defendants' actions violate the federal and California
25 laws asserted here;
26
27
28

- c. Whether Defendants caused third-party cookies to be placed, and third-party network requests to be transmitted, before the cookie consent banner was displayed;
- d. Whether the data transmitted to the Third Parties constitutes the “contents” of a communication under 18 U.S.C. § 2510(8) and Cal. Penal Code § 631(a);
- e. Whether the Third Parties acquired those communications contemporaneously with their transmission;
- f. Whether Defendants intercepted, or procured the interception of, those communications for the purpose of committing a criminal or tortious act within the meaning of 18 U.S.C. § 2511(2)(d);
- g. Whether Defendants’ access to and taking of data from Class members’ devices was “without permission” within the meaning of Cal. Penal Code § 502;
- h. 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.

108. **Typicality**: Plaintiff’s claims are typical of the proposed Classes. Like the proposed Classes, Plaintiff used the Website and rejected cookies, and Defendants nonetheless permitted the Third Parties to place cookies and to track and collect her Private Communications. There are no conflicts of interest between Plaintiff and the Classes.

109. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff’s claims are representative of the claims of the other members of the Classes. That is, Plaintiff and the members of the Classes sustained injuries and damages as a result of

Defendants' conduct. Plaintiff also has no interests antagonistic to those of the Classes, and Defendants have no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes and have the financial resources to do so. Neither Plaintiff nor her counsel have any conflicts with or interests adverse to the Classes.

110. **Superiority**: Class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, as joinder of all members of the Classes is impracticable. Individual litigation would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint as well as the risk of inconsistent adjudication. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Through a class action, economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

111. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definitions" based on facts learned through additional investigation and in discovery.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

INVASION OF PRIVACY

(On Behalf of Plaintiff & the California Subclass)

112. Plaintiff repeats and re-alleges all factual allegations contained in the foregoing paragraphs as if fully set forth herein.

113. Plaintiff brings this claim individually and on behalf of the members of the California Subclass against Defendant.

114. 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

1 expectation of privacy in the circumstances; and (iii) conduct by Defendants
2 constituting a serious invasion of privacy.

3 115. Plaintiff and Class members had legally protected privacy interests
4 under the following: (i) the California Invasion of Privacy Act, as alleged here; (ii)
5 the California Constitution, which guarantees Californians the right to privacy; (iii)
6 the California Wiretap Acts as alleged here; (iv) Cal. Penal Code § 484(a), which
7 prohibits the knowing theft or defrauding of property “by any false or fraudulent
8 representation or pretense;” (v) Plaintiff’s and Class members’ Fourth Amendment
9 right to privacy; (vi) the Federal Wiretap Act, 18 U.S.C. § 2510, et seq., as alleged
10 here; and (vii) the California Comprehensive Computer Data Access and Fraud Act,
11 Cal. Penal Code § 502, as alleged here. Defendants intruded upon these legally
12 protected privacy interests of Plaintiff and Class members.

13 116. Plaintiff and Class members had a reasonable expectation of privacy
14 because Defendants affirmatively promised users they could reject cookies and
15 tracking technologies before browsing the Website. Plaintiff and other Class
16 members used the Website and, when presented with Website’s consent banner,
17 rejected cookies. Plaintiff and other Class members reasonably expected that their
18 rejection of cookies and tracking technologies would be honored. That is, they
19 reasonably believed that Defendants would not permit the Third Parties to store and
20 send cookies and/or use other such tracking technologies on their devices while they
21 browsed the Website. Plaintiff and Class members also reasonably expected that, if
22 they rejected such cookies and/or tracking technologies, Defendants would not
23 permit the Third Parties to track and collect Plaintiff’s and Class members’ Private
24 Communications, including their browsing history, visit history, website interactions,
25 user input data, demographic information, interests and preferences, shopping
26 behaviors, device information, referring URLs, session information, user identifiers,
27 geolocation data, and IP address.
28

1 117. Such information (e.g., the Private Communications) is “personal
2 information” under California law, which defines personal information as including
3 “[c]ommercial information, including records of personal property, products or
4 services purchased, obtained, or considered, or other purchasing or consuming
5 histories or tendencies” and “Internet or other electronic network activity
6 information,” such as “browsing history, search history, and information regarding a
7 consumer’s interaction with an internet website, application, or advertisement.” Cal.
8 Civ. Code § 1798.140.

9 118. Defendants’ actions constituted a serious invasion of privacy.
10 Defendant, in violation of Plaintiff’s and other Class members’ reasonable
11 expectation of privacy and without their consent, permitted the Third Parties to use
12 cookies and other tracking technologies to collect, track, and compile users’ Private
13 Communications. The data that Defendants allowed the Third Parties to collect
14 enables the Third Parties to create consumer profiles containing detailed information
15 about a consumer’s behavior, preferences, and demographics; create audience
16 segments based on shared traits (such as “expectant parents,” “new mothers,” or
17 “baby product shoppers,” etc.); and perform targeted advertising and marketing
18 analytics. Further, the Third Parties share user data and/or the user profiles to
19 unknown parties to further their financial gain. The consumer profiles are and can be
20 used to further invade Plaintiff’s and users’ privacy, by allowing third parties to learn
21 intimate details of their lives, and target them for advertising and other purposes,
22 thereby harming them by depriving them of control over their personal information
23 and the ability to decide how it is shared or used.

24 119. Defendants’ actions invaded a zone of privacy protected by the Fourth
25 Amendment (i.e., one’s personal communications) and violated criminal laws on
26 wiretapping and invasion of privacy. By offering users a choice to reject cookies and
27 then ignoring its users’ preferences, Defendants committed a serious invasion of
28

1 privacy by deliberately undermining users' control over their personal data,
2 surreptitiously harvesting sensitive information despite explicit instructions to the
3 contrary, and fostering a false sense of security that led users to believe their
4 browsing activity would remain private when, in fact, it was being shared with the
5 Third Parties.

6 120. Defendants did not have a legitimate business interest in ignoring the
7 results of a choice (to reject cookies) that it presented to users.

8 121. These acts constitute an egregious breach of social norms that is highly
9 offensive. Defendants' intrusion into Plaintiff's privacy was also highly offensive to
10 a reasonable person.

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

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

18 124. Plaintiff and Class members seek punitive damages because
19 Defendants' actions—which were malicious, oppressive, willful—were calculated
20 to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's
21 and Class members' rights and Plaintiff's and Class members' rejection of the
22 Website's use of cookies. Punitive damages are warranted to deter Defendants from
23 engaging in future misconduct.

24 //

25 //

26 //

27 //

1 **SECOND CAUSE OF ACTION**

2 **INTRUSION UPON SECLUSION**

3 **(On Behalf of Plaintiff & the California Subclass)**

4 125. Plaintiff repeats and re-alleges all factual allegations contained in the
5 foregoing paragraphs as if fully set forth herein.

6 126. Plaintiff brings this claim individually and on behalf of the members of
7 the California Subclass.

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

12 128. As described above, Defendants intruded into a place (its Website) and
13 a conversation (the Private Communications between Plaintiff and Class members
14 and Defendant) where Plaintiff and Class members had a reasonable expectation of
15 privacy.

16 129. Defendants explicitly offered users the option to reject cookies—a clear
17 acknowledgment that users could choose not to be tracked. By accepting this offer
18 and rejecting cookies, users communicated their intent to browse privately and
19 without third-party surveillance. Defendants’ decision to ignore those preferences
20 and allow third-party tracking anyway meant that it enabled outsiders to access and
21 monitor users’ interactions with the Website—Private Communications that users
22 reasonably expected would remain confidential. This surreptitious override of user
23 consent invaded the private digital space users were led to believe was protected.

24 130. Defendants placed the Third Parties in the middle of communications to
25 which they were not invited, welcomed, or authorized. In other words, Defendants
26 allowed Third Parties to intercept and read communications without permission.
27
28

1 131. Plaintiff and the Class members had an objectively reasonable
2 expectation of privacy surrounding their Private Communications on the Website
3 based on Defendants' promise that users could reject cookies, the fact that they chose
4 to reject cookies, as well as state criminal and civil laws designed to protect
5 individual privacy.

6 132. Defendants' conduct is highly offensive because it knowingly bypassed
7 users' privacy choices, exposed Private (and sensitive) Communications, and
8 violated reasonable expectations of privacy.

9 133. Defendants' conduct was intentional. The Website's behavior is the
10 direct result of code Defendants either developed, implemented, or authorized. When
11 a user rejects some or all cookies on a cookie banner, that input triggers specific logic
12 in the site's code—logic that determines whether tracking technologies are blocked
13 or allowed. If cookies continue to be set after rejection, it means the website's code
14 is configured to permit that behavior. Website owners are responsible for reviewing
15 and testing their site's functionality, including privacy features. There are a number
16 of tools available (including tools more powerful than the Developer Tools
17 functionality in the Chrome browser) to indicate when cookies are being deployed
18 and under what conditions.

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

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

26 136. Plaintiff and Class members seek punitive damages because
27 Defendants' actions—which were malicious, oppressive, willful—were calculated
28

1 to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's
 2 and Class members' rights and Plaintiff's and Class members' rejection of the
 3 Website's use of cookies. Punitive damages are warranted to deter Defendants from
 4 engaging in future misconduct.

5 **THIRD CAUSE OF ACTION**

6 **VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT**

7 **Cal. Penal Code § 631**

8 **(On Behalf of Plaintiff & the California Subclass)**

9 137. Plaintiff repeats and re-alleges all factual allegations contained in the
 10 foregoing paragraphs as if fully set forth herein.

11 138. Plaintiff brings this claim individually and on behalf of the members of
 12 the California Subclass against Defendant.

13 139. The California Legislature has declared "that advances in science and
 14 technology have led to the development of new devices and techniques for the
 15 purpose of eavesdropping upon private communications and that the invasion of
 16 privacy resulting from the continual and increasing use of such devices and
 17 techniques has created a serious threat to the free exercise of personal liberties and
 18 cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

19 140. California Penal Code § 631(a) imposes liability on four distinct
 20 categories of conduct. It provides, in pertinent part: "Any person who, by means of
 21 any machine, instrument, or contrivance, or in any other manner . . . willfully and
 22 without the consent of all parties to the communication, or in any unauthorized
 23 manner, reads, or attempts to read, or to learn the contents or meaning of any
 24 message, report, or communication while the same is in transit or passing over any
 25 wire, line, or cable, or is being sent from, or received at any place within this state;
 26 or who uses, or attempts to use, in any manner, or for any purpose, or to communicate
 27 in any way, any information so obtained . . . , or who aids, agrees with, employs, or
 28 conspires with any person or persons to unlawfully do, or permit, or cause to be done

1 any of the acts or things mentioned above in this section, is punishable by a fine not
 2 exceeding two thousand five hundred dollars”

3 141. Section 631(a) is not limited to phone lines, but also applies to new
 4 technologies such as computers, the Internet, and email. *See Matera v. Google Inc.*,
 5 2016 WL 8200619 (N.D. Cal. Aug. 12, 2016); *see also Bradley v. Google, Inc.*, 2006
 6 WL 3798134 (N.D. Cal. Dec. 22, 2006); *Javier v. Assurance IQ, LLC*, 2022 WL
 7 1744107, at *1 (9th Cir. May 31, 2022).

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

- 13 a. Intentionally taps, or makes any unauthorized connection,
 14 whether physically, electrically, acoustically, inductively or
 15 otherwise, with any telegraph or telephone wire, line, cable, or
 16 instrument, including the wire, line, cable, or instrument of any
 17 internal telephonic communication system;
- 18 b. Willfully and without the consent of all parties to the
 19 communication, or in any unauthorized manner, reads or attempts
 20 to read or learn the contents or meaning of any message, report,
 21 or communication while the same is in transit or passing over any
 22 wire, line or cable or is being sent from or received at any place
 23 within this state;
- 24 c. Uses, or attempts to use, in any manner, or for any purpose, or to
 25 communicate in any way, any information so obtained.

26 143. Defendants did all of those. In other words, it engaged in each type of
 27 prohibited conduct described above. The means and methods by which Defendants
 28

1 did so were the same: it offered Plaintiff and Class members the choice to reject
2 cookies. But after users exercised that choice, Defendants ignored their selections
3 and continued to deploy third-party cookies and tracking technologies which
4 transmitted Plaintiff's and Class members' Private Communications with
5 Defendant—such as what they searched for, clicked on, and viewed—to the Third
6 Parties without users' knowledge or consent.

7 144. By configuring the Website in this manner,

- 8 a. Defendants intentionally aided, agreed with, and/or conspired
9 with the Third Parties to electrically and otherwise wiretap and
10 make unauthorized connections of Private Communications
11 intended to be between Plaintiff and Class members, on one hand,
12 and Defendants on the other. It did so by embedding Third Party
13 tracking code into its Website that caused users' browsers to
14 initiate real-time data transmissions to the Third Parties during
15 user interactions with the site, enabling those entities to intercept,
16 record, and analyze the substance of users' Private
17 Communications without consent.
- 18 b. Defendants willfully and without the consent of Plaintiff and
19 Website users also aided, agreed with, and/or conspired with the
20 Third Parties to read, attempt to read, or learn the contents or
21 meaning of Private Communications while in transit and passing
22 over the Internet in an unauthorized manner while the electronic
23 communications were in transit or were being sent from or
24 received at any place within California.
- 25 c. Defendants aided, agreed with, and/conspired with the Third
26 Parties to use or attempt to use the data that it surreptitiously
27 obtained from Plaintiff and Class members.
28

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

9 146. Defendants is a “person” within the meaning of California Penal Code
10 § 631.

11 147. Each of the Third Parties is a separate legal entity and not a passive
12 recipient of the Private Communications. Each had the capability to use the
13 wiretapped information for its own purposes and, as alleged above, did in fact use
14 the wiretapped information for their own business purposes.

15 148. Defendants cannot show it had the consent. Plaintiff and Class members
16 did not provide their prior consent to the Third Parties’ intentional access,
17 interception, reading, learning, recording, collection, and usage of Plaintiff’s and
18 Class members’ electronic communications. Nor did Plaintiff and Class members
19 provide their prior consent to Defendants aiding, agreeing with, or otherwise enabling
20 the Third Parties’ conduct. On the contrary, Plaintiff and Class members expressly
21 declined to allow Third Parties’ cookies and tracking technologies to access,
22 intercept, read, learn, record, collect, and use Plaintiff’s and Class members’
23 electronic communications by choosing to reject cookies in the consent banner.

24 149. The wiretapping of Plaintiff and Class members occurred in California,
25 where Plaintiff and Class members accessed the Website and where the Third
26 Parties—as enabled by Defendant—routed Plaintiff’s and Class members’ electronic
27 communications to Third Parties’ servers. Among other things, the cookies, as well
28

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

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

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

19 152. Unless enjoined, Defendants will continue to commit the illegal acts
20 alleged herein including, but not limited to, permitting the Third Parties to access,
21 intercept, read, learn, record, collect, and use Plaintiff's and Class members'
22 electronic Private Communications with Defendant. Plaintiff, Class members, and
23 the general public continue to be at risk because Plaintiff, Class members, and the
24 general public frequently use the internet to search for information and content
25 related to pregnancy, parenting, and children's health. Plaintiff, Class members, and
26 the general public continue to desire to use the internet for that purpose. Plaintiff,
27 Class members, and the general public have no practical way to know if their request
28

1 to reject cookies and tracking technologies will be honored and/or whether
 2 Defendants will permit the Third Parties to access, intercept, read, learn, record,
 3 collect, and use Plaintiff's and Class members' electronic Private Communications
 4 with Defendant. Further, Defendants has already permitted the Third Parties to
 5 access, intercept, read, learn, record, collect, and use Plaintiff's and Class members'
 6 electronic Private Communications with Defendants and will continue to do so unless
 7 and until enjoined.

8 **FOURTH CAUSE OF ACTION**

9 **VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT** 10 **Cal. Penal Code § 632** 11 **(On Behalf of Plaintiff & the California Subclass)**

12 153. Plaintiff repeats and re-alleges all factual allegations contained in the
 13 foregoing paragraphs as if fully set forth herein.

14 154. Plaintiff brings this claim individually and on behalf of the members of
 15 the California Subclass against Defendant.

16 155. California Penal Code § 632(a) provides that:
 17 [E]very person who, intentionally and without the consent
 18 of all parties to a confidential communication, uses an
 19 electronic amplifying or recording device to eavesdrop
 20 upon or record the confidential communication, whether
 the communication is carried on among the parties in the
 presence of one another or by means of a telegraph,
 telephone, or other device, except a radio, shall be
 punished[.]

21 156. California Penal Code § 632(c) defines "confidential communication"
 22 as "any communication carried on in circumstances as may reasonably indicate that
 23 any party to the communication desires it to be confined to the parties thereto, but
 24 excludes a communication made in a public gathering or in any legislative, judicial,
 25 or other public proceeding in which the public is entitled to attend, or in any other
 26 circumstance in which the parties to the communication may reasonably expect that
 27 the communication may be overheard or recorded."
 28

1 157. The Private Communications between Plaintiff and California Subclass
2 members, on the one hand, and Defendant, on the other, constitute “confidential
3 communications” within the meaning of Section 632(c) because:

- 4 a. Defendants themselves created the circumstances that made these
5 communications confidential. Defendants chose to present each
6 California visitor with a banner disclosing that it shares
7 information about the way users interact with the Website—
8 “including health information interests”—with its advertising and
9 analytics partners, and representing that a user who did not wish
10 to consent could click “Do Not Consent.” Plaintiff and California
11 Subclass members clicked “Do Not Consent.” A party who is told
12 by the other party to a communication that she may confine that
13 communication to the two of them, and who accepts that offer, is
14 communicating in “circumstances as may reasonably indicate”
15 that she desires it be so confined. Cal. Penal Code § 632(c).
16 Defendants solicited that understanding, obtained the benefit of
17 it, and cannot now disclaim it;
- 18 b. Defendants’ representation was a source of the confidentiality.
19 Whatever a user might otherwise assume about an ordinary
20 website, this Website told her she could shut off the sharing. Her
21 expectation that the communications would be confined to herself
22 and Defendants was therefore not merely subjective but was the
23 expectation Defendants’ own words invited;
- 24 c. The communications concerned users’ fertility, pregnancies,
25 pregnancy stage, children’s ages, and children’s health—among
26 the most sensitive categories of personal information, and
27
28

1 subjects as to which users reasonably expect confidentiality and
2 would not knowingly broadcast to third-party advertisers;

3 d. Defendants' Privacy Policy represented that Defendants
4 maintained consent records and would honor users' elections,
5 reinforcing the reasonable expectation that those communications
6 would be confined to the user and Defendant;

7 e. The communications were not made in a public gathering or in
8 any legislative, judicial, or other public proceeding in which the
9 public is entitled to attend; and

10 f. Having rejected cookies and tracking technologies, Plaintiff and
11 California Subclass members had no reason to expect that their
12 communications with the Website would be overheard or
13 recorded by the Third Parties.

14 158. Defendants intentionally used electronic recording devices—
15 specifically, the Third Parties' cookies, pixels, and corresponding software code
16 embedded within the Website—to eavesdrop upon and record these confidential
17 communications. Defendants is liable under Section 632 on either of two independent
18 grounds, pleaded in the alternative. First, Defendants intentionally used an electronic
19 recording device to record these confidential communications. Second, and in the
20 alternative, Defendants aided, assisted, and abetted the Third Parties' eavesdropping
21 upon those confidential communications.

22 159. The Third Parties' cookies and corresponding software code constitute
23 "electronic amplifying or recording device[s]" within the meaning of Section 632(a)
24 because they are specifically designed to capture, record, and transmit users'
25 interactions and communications in real time for advertising, analytics, and
26 behavioral tracking purposes.

1 160. Defendants intentionally implemented and activated these recording
2 technologies on the Website with knowledge that they would capture and record
3 users' confidential communications, including their browsing history, visit history,
4 website interactions, user input data, interests and preferences, and the specific
5 pregnancy- and parenting-related content they chose to view.

6 161. Defendants' recording of Plaintiff's and California Subclass members'
7 confidential communications was accomplished without the consent of all parties to
8 the communication, specifically:

- 9 a. Plaintiff and Class members never consented to having their
10 Private Communications recorded by third-party advertising and
11 analytics companies;
- 12 b. Defendants never obtained consent before deploying the Third
13 Parties' recording technologies, and in fact users affirmatively
14 declined by selecting "Do Not Consent";
- 15 c. Users were not informed that their communications with the
16 Website would continue to be recorded and transmitted to the
17 Third Parties after they rejected cookies;
- 18 d. No clear and conspicuous notice was provided regarding the
19 scope and nature of the recording that continued notwithstanding
20 users' rejection of cookies; and
- 21 e. The recording began immediately upon the user's arrival at the
22 Website, before the user had any opportunity to review the
23 Privacy Policy or to exercise the cookie choice Defendants
24 offered.

25 162. Defendants' conduct was undertaken intentionally and with knowledge
26 that the Third Parties' recording technologies would capture and record confidential
27 communications without the consent of all parties to those communications.
28

1 163. The confidential communications that were unlawfully recorded include
2 sensitive information concerning users' fertility, pregnancies, children, and health-
3 related interests, which Plaintiff and California Subclass members disclosed with a
4 reasonable expectation of privacy.

5 164. As a direct and proximate result of Defendants' violations of Section
6 632, Plaintiff and Class members have suffered harm, including invasion of their
7 privacy rights, diminution in the value of their Private Communications, and loss of
8 control over their sensitive personal information.

9 165. Unless enjoined and restrained by this Court, Defendants will continue
10 to commit these violations. Plaintiff and Class members have a reasonable fear that
11 their confidential communications will continue to be unlawfully recorded if they use
12 the Website.

13 166. Pursuant to California Penal Code § 637.2, Plaintiff and Class members
14 are entitled to:

- 15 a. A preliminary and permanent injunction prohibiting Defendants
16 from continuing its unlawful recording of confidential
17 communications;
- 18 b. Statutory damages of the greater of \$5,000, or three times the
19 amount of actual damages, for each violation;
- 20 c. Punitive damages for Defendants' willful and egregious
21 violations of Plaintiff's and Class members' privacy; and
- 22 d. Any other relief the Court deems proper.

23 167. Plaintiff and Class members seek all available remedies under
24 California Penal Code § 632 and related provisions for Defendants' unlawful
25 recording of their confidential communications and for Defendants' aiding and
26 abetting of the Third Parties' eavesdropping upon them.

27 //
28

1 **FIFTH CAUSE OF ACTION**

2 **VIOLATION OF THE FEDERAL WIRETAP ACT**
 3 **18 U.S.C. § 2510, et seq.**
 4 **(On Behalf of Plaintiff & the Nationwide Class)**

5 168. Plaintiff repeats and re-alleges all factual allegations contained in the
 6 foregoing paragraphs as if fully set forth herein.

7 169. Plaintiff brings this claim individually and on behalf of the members of
 8 the Nationwide Class against Defendant.

9 170. The Federal Wiretap Act, as amended by the Electronic
 10 Communications Privacy Act, imposes liability on any person who “intentionally
 11 intercepts, endeavors to intercept, or procures any other person to intercept or
 12 endeavor to intercept, any wire, oral, or electronic communication,” 18 U.S.C. §
 13 2511(1)(a), and on any person who intentionally discloses or uses the contents of an
 14 electronic communication knowing or having reason to know that it was obtained
 15 through an unlawful interception, id. § 2511(1)(c)–(d). Section 2520(a) affords a civil
 16 remedy to any person whose electronic communication is intercepted, disclosed, or
 17 intentionally used in violation of the chapter.

18 171. Defendants is a “person” within the meaning of 18 U.S.C. § 2510(6).

19 172. Plaintiff’s and Class members’ communications with the Website were
 20 “electronic communication[s]” within the meaning of 18 U.S.C. § 2510(12).

21 173. The Third Parties’ cookies, tags, pixels, and corresponding software
 22 code are “device[s]” within the meaning of 18 U.S.C. § 2510(5).

23 174. The information acquired by the Third Parties constitutes the “contents”
 24 of those communications—“any information concerning the substance, purport, or
 25 meaning of [the] communication,” 18 U.S.C. § 2510(8). Those contents included the
 26 full URLs of the pregnancy- and parenting-related pages Plaintiff and Class members
 27 chose to view; the search terms they typed into the Website’s search bar, transmitted
 28 to the Third Parties in the Referer header; the values they submitted to the Pregnancy

1 Due Date Calculator and Ovulation Calculator; and the cust_params values encoding
2 content category, pregnancy stage, and child age.

3 175. The Third Parties' acquisition of those contents was an "intercept[ion]"
4 within the meaning of 18 U.S.C. § 2510(4) because it was contemporaneous with
5 transmission. As alleged above, the Third Parties read, transform, deduplicate,
6 validate, and analyze the payload as it arrives and before it is committed to storage.

7 176. Defendants acted intentionally. Defendants wrote, approved, or
8 authorized the code that causes the Third Parties' tags to load; Defendants configured
9 the consent-management platform that determines whether those tags fire after a user
10 refuses consent; and Defendants monitored the Third Parties' analytics and
11 advertising dashboards, through which the continued flow of user data was visible to
12 Defendant.

13 177. Defendants cannot invoke the party exception of 18 U.S.C. §
14 2511(2)(d). That exception is unavailable where the communication "is intercepted
15 for the purpose of committing any criminal or tortious act in violation of the
16 Constitution or laws of the United States or of any State." Defendants intercepted, and
17 procured the Third Parties to intercept, Plaintiff's and Class members'
18 communications for the purpose of committing at least the following criminal or
19 tortious acts, each independent of the interception itself:

- 20 a. Intentional misrepresentation, negligent misrepresentation, and
21 common-law fraud and deceit. Defendants told users they could
22 refuse the Website's use of cookies and the sharing of their
23 health-related interests with advertising and analytics partners.
24 That representation was false. Defendants made it in order to
25 induce users to keep browsing and to keep disclosing information
26 about their fertility, pregnancies, and children—the very
27 information Defendants then monetized;
28

- b. Intrusion upon seclusion and invasion of privacy under California law;
- c. Violation of California Penal Code § 502; and
- d. Unjust enrichment.

178. A website operator's misrepresentations in its own consent disclosures and privacy policy can supply the predicate tort for the crime-tort exception. *See, e.g., Smith v. Rack Room Shoes, Inc.*, 2025 WL 2210002 (N.D. Cal. Aug. 4, 2025).

179. Defendants' tortious purpose is independent of, and not merely coextensive with, the interception itself. Defendants did not simply route data to its vendors. Defendants first told its users they could stop that routing; obtained the commercial benefit of their continued engagement and continued disclosure on the strength of that assurance; and routed the data anyway. The misrepresentation was the means by which the interception was accomplished and enlarged.

180. Neither Plaintiff nor Class members consented to the interception. They were asked whether they consented and they answered no.

181. Pursuant to 18 U.S.C. § 2520(b) and (c)(2), Plaintiff and Class members are entitled to injunctive and declaratory relief; the greater of (i) the sum of their actual damages and any profits Defendants realized as a result of the violation or (ii) statutory damages of \$100 per day for each day of violation or \$10,000, whichever is greater; punitive damages; and reasonable attorneys' fees and costs.

SIXTH CAUSE OF ACTION

FRAUD, DECEIT, AND/OR MISREPRESENTATION (On Behalf of Plaintiff & the California Subclass)

182. Plaintiff repeats and re-alleges all factual allegations contained in the foregoing paragraphs as if fully set forth herein.

183. Plaintiff brings this claim individually and on behalf of the members of the California Subclass against Defendant.

1 184. As alleged in detail above, Defendants made false representations and
2 material omissions of fact to Plaintiff and Class members concerning the ability to
3 reject cookies.

4 185. These representations were false.

5 186. When Defendants made these misrepresentations, it knew that they were
6 false at the time that they made them and/or acted recklessly in making the
7 misrepresentations.

8 187. Defendants intended that Plaintiff and Class members rely on these
9 representations and Plaintiff read and reasonably relied on them.

10 188. Class-wide reliance can be inferred because Defendants'
11 representations were material. A reasonable consumer would consider them
12 important in deciding whether to reject cookies.

13 189. Defendants' actions were a substantial factor and proximate cause in
14 causing damages and losses to Plaintiff's and Class members' property right to
15 control the dissemination and use of their personal information and communications.

16 190. Plaintiff and the Class members were injured as a direct and proximate
17 result of Defendants' conduct because (a) they would not have used the Website had
18 they known that they could not reject cookies or (b) they would have used the
19 Website differently.

20 SEVENTH CAUSE OF ACTION

21 UNJUST ENRICHMENT

22 (On behalf of Plaintiff & the California Subclass)

23 191. Plaintiff and the California Subclass members incorporate the foregoing
24 allegations as if fully set forth herein.

25 192. Plaintiff brings this cause of action on behalf of herself and members of
26 the California Subclass.
27
28

193. As alleged in detail above, Defendants' false and misleading promise to allow users to reject cookies caused Plaintiff and Class members to use the Website and communicate with it, revealing information about themselves that Defendants and Third Parties could use, monetize, and profit from.

194. In this way, Defendants received a direct and unjust benefit at Plaintiff's expense.

195. Plaintiff and the Class pleads this claim in the alternative to their other claims.

196. 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 they occupied prior to having their Private Communications tracked and collected by the Third Parties.

EIGHTH CAUSE OF ACTION

BREACH OF CONTRACT

(On behalf of Plaintiff & the Nationwide Class)

197. Plaintiff and the California Subclass members incorporate the foregoing allegations as if fully set forth herein.

198. Defendants' relationship with its users is governed by the popup cookie consent banner, which represents that users may decline consent to the Website's use of cookies and associated data sharing: "Please click I Consent below to give us permission to do this. If you do not wish to consent please click Do Not Consent." It then allowed users to decline that consent by clicking the "Do Not Consent" button.

199. This is an enforceable promise that Defendants made to Plaintiff and Class members.

200. As described in detail above, Defendants breached these duties and violated these promises.

1 201. At all relevant times and in all relevant ways, Plaintiff and Class
2 members performed their obligations under the popup cookie consent banner or were
3 excused from performance of such obligations through the unknown and unforeseen
4 conduct of others.

5 202. As a direct and proximate result of Defendants' breach of contract,
6 Plaintiff and Class members did not receive the full benefit of the bargain, and instead
7 received services from Defendants that were less valuable than described in the
8 Privacy Policy. Plaintiff and Class members, therefore, were damaged in an amount
9 at least equal to the difference in value between that which was promised and
10 Defendants' partial, deficient, and/or defective performance.

11 203. As a direct consequence of the breaches of contract and violations of
12 promises described above, Plaintiff and Class members seek nominal damages,
13 compensatory damages, consequential damages, and any other just relief.

14 NINTH CAUSE OF ACTION

15 NEGLIGENT MISREPRESENTATION 16 (On behalf of Plaintiff & the California Subclass)

17 204. Plaintiff and the California Subclass members incorporate the foregoing
18 allegations as if fully set forth herein.

19 205. Plaintiff brings this cause of action on behalf of herself and the
20 California Subclass.

21 206. As described above, Defendants represented to Plaintiff and California
22 Subclass members, through its popup cookie consent banner and its Privacy Policy,
23 that they could decline the Website's use of cookies and the sharing of information
24 about the way they interact with the Website—including health information
25 interests—with Defendants' advertising and analytics partners.

26 //

27 //

1 207. Those representations concerned past or existing material facts about
2 how the Website was configured and how it would treat a user's rejection of cookies,
3 and they were false when made.

4 208. Defendants had no reasonable ground for believing the representations
5 to be true. Defendants designed, implemented, or authorized the software code that
6 governs the Website's response to a user's cookie selection, and it had both the ability
7 and the responsibility to test whether that code honored a rejection. Had Defendants
8 exercised reasonable care in reviewing or testing its own Website, it would have
9 discovered that third-party cookies and tracking technologies continued to be placed
10 on users' devices and transmitted to the Third Parties after users selected "Do Not
11 Consent."

12 209. Defendants made the representations intending that Plaintiff and
13 California Subclass members rely on them by continuing to browse the Website and
14 by submitting information about their fertility, pregnancies, and children.

15 210. Plaintiff and California Subclass members justifiably relied on the
16 representations. Plaintiff reviewed the popup cookie consent banner and the Privacy
17 Policy, selected "Do Not Consent," and only then continued to browse the Website.
18 A reasonable consumer would rely on a privacy representation made by the operator
19 of the website on which it appears, and would have no practical means of verifying
20 that representation absent specialized developer tools.

21 211. As a direct and proximate result of Defendants' negligent
22 misrepresentations, Plaintiff and California Subclass members were damaged,
23 including through the loss of their property right to control the dissemination and use
24 of their Private Communications, the diminution in value of those Private
25 Communications, and their use of the Website on terms they would not have accepted
26 had the truth been disclosed.

27 //
28

1 **TENTH CAUSE OF ACTION**

2 **INTENTIONAL MISREPRESENTATION**
3 **(On behalf of Plaintiff & the California Subclass)**

4 212. Plaintiff and the California Subclass members incorporate the foregoing
5 allegations as if fully set forth herein.

6 213. Plaintiff brings this cause of action on behalf of herself and the
7 California Subclass, and in the alternative to the Ninth Cause of Action *supra*.

8 214. As described above, Defendants represented to Plaintiff and California
9 Subclass members, through its popup cookie consent banner and its Privacy Policy,
10 that they could decline the Website's use of cookies and the sharing of information
11 about the way they interact with the Website—including health information
12 interests—with Defendants' advertising and analytics partners.

13 215. Those representations were false when made. Even after users selected
14 "Do Not Consent," Defendants continued to cause third-party cookies and tracking
15 technologies to be placed on their devices and transmitted to the Third Parties, along
16 with their Private Communications.

17 216. Defendants knew the representations were false when it made them, or
18 made them recklessly and without regard for their truth. Defendants controlled the
19 software code of its Website and the third-party tags it deployed, and represented in
20 its Privacy Policy that it maintained "[c]onsent records" documenting users'
21 elections. Defendants nonetheless continued to cause third-party cookies to be placed
22 and transmitted after users rejected them.

23 217. Defendants made the representations with the intent to deceive Plaintiff
24 and California Subclass members and to induce their reliance—specifically, to
25 induce them to continue browsing the Website and disclosing information about their
26 fertility, pregnancies, and children, which Defendants and the Third Parties could
27 then use, monetize, and profit from.
28

1 218. Plaintiff and California Subclass members justifiably relied on the
 2 representations, and class-wide reliance may be inferred because the representations
 3 were material. A reasonable consumer would consider a representation about whether
 4 tracking can be declined important in deciding whether to browse the Website and
 5 what information to disclose.

6 219. As a direct and proximate result of Defendants' intentional
 7 misrepresentations, Plaintiff and California Subclass members were damaged,
 8 including through the loss of their property right to control the dissemination and use
 9 of their Private Communications and the diminution in value of those Private
 10 Communications. Plaintiff and California Subclass members further seek punitive
 11 damages because Defendants' conduct was malicious, oppressive, and willful, and
 12 was undertaken in conscious disregard of their rights and of their express rejection
 13 of the Website's use of cookies.

14 **ELEVENTH CAUSE OF ACTION**

15 **VIOLATION OF THE CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND** 16 **FRAUD ACT, CAL. PENAL CODE § 502**

17 **(On Behalf of Plaintiff & the California Subclass)**

18 220. Plaintiff repeats and re-alleges all factual allegations contained in the
 19 foregoing paragraphs as if fully set forth herein.

20 221. Plaintiff brings this claim individually and on behalf of the members of
 21 the California Subclass against Defendant.

22 222. The Legislature enacted Section 502 to "expand the degree of protection
 23 afforded to individuals, businesses, and governmental agencies from tampering,
 24 interference, damage, and unauthorized access to lawfully created computer data and
 25 computer systems." Cal. Penal Code § 502(a). Section 502(e)(1) affords a civil action
 26 to any "owner or lessee of the computer, computer system, computer network,
 27 computer program, or data who suffers damage or loss by reason of a violation of
 28 any of the provisions of subdivision (c)."

1 223. Plaintiff and California Subclass members are the owners or lessees of
2 the computers, computer systems, and computer networks at issue—their own
3 personal computers, smartphones, tablets, and browsers—and of the data residing on
4 and generated by those devices. Those devices are “computer[s],” “computer
5 system[s],” and “computer network[s]” within the meaning of Cal. Penal Code §
6 502(b)(1)–(5), and the cookies, identifiers, and browsing and interaction records at
7 issue are “data” within the meaning of § 502(b)(8).

8 224. Defendants violated Cal. Penal Code § 502(c)(1) by knowingly
9 accessing and, without permission, taking, copying, and making use of data from
10 Plaintiff’s and California Subclass members’ computers, computer systems, and
11 computer networks in order to execute a scheme to deceive and to wrongfully obtain
12 data.

13 225. Defendants violated Cal. Penal Code § 502(c)(2) by knowingly
14 accessing and, without permission, taking, copying, and making use of data from
15 Plaintiff’s and California Subclass members’ computers, computer systems, and
16 computer networks.

17 226. Defendants violated Cal. Penal Code § 502(c)(3) by knowingly and
18 without permission using, and causing to be used, computer services—including the
19 processing capacity, storage, and network connections of Plaintiff’s and California
20 Subclass members’ devices, which Defendants conscripted to store the Third Parties’
21 cookies and to execute the Third Parties’ code.

22 227. Defendants violated Cal. Penal Code § 502(c)(6) by knowingly and
23 without permission providing, and assisting in providing, a means of accessing
24 Plaintiff’s and California Subclass members’ computers, computer systems, and
25 computer networks to the Third Parties.

26 //

27 //

1 228. Defendants violated Cal. Penal Code § 502(c)(7) by knowingly and
2 without permission accessing, and causing to be accessed, Plaintiff's and California
3 Subclass members' computers, computer systems, and computer networks.

4 229. Defendants' access and taking were "without permission." Section 502
5 does not require the circumvention of a technical barrier; it requires knowing access
6 together with a taking, copying, or use of data without permission. *See Greenley v.*
7 *Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023); *Esparza v. Kohl's, Inc.*, 723
8 F. Supp. 3d 934 (S.D. Cal. 2024). Here permission was not merely absent—it was
9 solicited and expressly refused. Defendants presented Plaintiff and California
10 Subclass members with a binary choice, received their answer, and proceeded as
11 though they had answered the other way. A defendant that asks for permission, is
12 told no, and acts anyway has acted without permission in the most literal sense the
13 statute admits.

14 230. Defendants acted knowingly. Defendants controlled the Website's
15 software code and the third-party tags it deployed; configured the consent-
16 management platform that governs whether those tags fire after a refusal; represented
17 in its Privacy Policy that it maintained "[c]onsent records" of each user's election;
18 and reviewed the Third Parties' reporting dashboards, in which the continued flow
19 of data from refusing users was apparent.

20 231. Plaintiff and California Subclass members suffered damage and loss
21 within the meaning of Cal. Penal Code § 502(e)(1), including: the loss of the value
22 of their Private Communications, which Defendants and the Third Parties monetized;
23 the loss of their property right to control the dissemination and use of those
24 communications; the consumption of their devices' storage, processing capacity,
25 battery, and bandwidth to store the Third Parties' cookies and execute the Third
26 Parties' code; and the impairment of the integrity of their devices and data.

1 232. Plaintiff and California Subclass members are entitled to compensatory
2 damages and injunctive and other equitable relief pursuant to Cal. Penal Code §
3 502(e)(1); to reasonable attorneys' fees pursuant to § 502(e)(2); and, because
4 Defendants' violation was willful, to punitive or exemplary damages pursuant to §
5 502(e)(4).

6
7 **PRAYER FOR RELIEF**

8 WHEREFORE, Plaintiff, individually and on behalf of all others similarly
9 situated, respectfully requests that this Court enter judgment against Defendants and
10 in favor of Plaintiff and the Classes, and grant the following relief:

- 11 a. For an order certifying the Classes and naming Plaintiff as the
12 representatives of the putative Classes and Plaintiff's attorneys as
13 Class Counsel to represent the putative Class members;
- 14 b. For an order declaring that the Defendants' conduct violates the
15 statutes and laws referenced herein;
- 16 c. For an order finding in favor of Plaintiff and the Classes on all
17 counts asserted herein;
- 18 d. For damages, treble damages, and punitive damages where
19 applicable in an amount to be determined by the Court and/or
20 jury;
- 21 e. For prejudgment interest on all amounts awarded;
- 22 f. For injunctive relief, restitution, and disgorgement, as pleaded or
23 as the Court may deem proper;
- 24 g. For an order awarding Plaintiff and the putative Classes their
25 reasonable attorneys' fees and expenses and cost of suit; and
- 26 h. Any additional relief that the Court deems reasonable and just.

27 **JURY TRIAL DEMANDED**

28 Plaintiff demands a trial by jury for all issues so triable.

1 Dated: September 22, 2026

Respectfully Submitted,

3 /s/ Victor J. Sandoval

4 Victor J. Sandoval, SBN 344461
ALMEIDA LAW GROUP LLC
5 3415 S. Sepulveda Blvd. Suite 1121
Los Angeles, California 90034
6 562-534-5907
victor@almeidalawgroup.com

7 *Counsel for Plaintiff & the Proposed Classes*