

1 Reuben D. Nathan, Esq. (SBN 208436)

2 **NATHAN & ASSOCIATES, APC**

3 2901 W. Coast Hwy., Suite 200

4 Newport Beach, CA 92663

5 Office: (949) 270-2798

6 Email: rnathan@nathanlawpractice.com

7 Ross Cornell, Esq. (SBN 210413)

8 **LAW OFFICES OF ROSS CORNELL, APC**

9 40729 Village Dr., Suite 8 - 1989

10 Big Bear Lake, CA 92315

11 Office: (562) 612-1708

12 Email: rc@rosscornelllaw.com

13 Attorneys for Plaintiff: MICHAEL HANSON

14 **UNITED STATES DISTRICT COURT**

15 **CENTRAL DISTRICT OF CALIFORNIA**

16 MICHAEL HANSON, on behalf of
17 himself and all similarly situated
18 persons,

19 Plaintiff,

20 v.

21 BONANZA WORLDWIDE LLC, a
22 Florida limited liability company,

23 Defendant.

Case No:

COMPLAINT

1. Cal. Penal Code § 638.51

2. Cal. Bus. & Prof. Code § 17200, *et seq.*

CLASS ACTION

I. NATURE OF THE ACTION

1
2 1. Defendant BONANZA WORLDWIDE LLC, a Florida limited liability
3 company (referred to herein as “Defendant” or “BONANZA”) owns and operate a
4 website, www.bonanza.com (the “Website”).

5 2. This is a class action lawsuit brought by Plaintiff on behalf of himself
6 and on behalf of all California residents who have accessed the Website.

7 3. Plaintiff MICHAEL HANSON files this class action complaint on behalf
8 of himself and all others similarly situated (the “Class Members”) against Defendant.
9 Plaintiff brings this action based upon personal knowledge of the facts pertaining to
10 him, and on information and belief as to all other matters, by and through the
11 investigation of undersigned counsel.

12 4. A pixel tracker, also known as a web beacon, is a tracking mechanism
13 embedded in a website that monitors user interactions. It typically appears as a small,
14 transparent 1x1 image or a lightweight JavaScript snippet that activates when a webpage
15 is loaded or a user performs a tracked action.

16 5. When triggered, the pixel transmits data from the user’s browser to a
17 third-party server. This data typically includes page views, session duration, referrer
18 URLs, IP address, browser and device details, and other interaction metadata.

19 6. When users visit the Website, Defendant causes tracking technologies to
20 be installed, executed, embedded, or injected in visitors’ browsers. These include, but
21 are not limited to, the following:

- 22 • Google Ads / DoubleClick Tracker
- 23 • Facebook Pixel Tracker
- 24 • Bing/Microsoft Ads Tracker

25 7. Other third party software trackers used by Defendant on the Website
26 include the Klaviyo, Pinterest and Criteo Trackers, among others. The third parties who
27 operate the trackers use pieces of User Information (defined below) collected via the
28 Website as described herein for their own independent purposes tied to broader

1 advertising ecosystems, profiling, and data monetization strategies that go beyond
2 Defendant's direct needs for their own financial gain. The above-listed trackers are
3 referred to herein collectively as the "Trackers."

4 8. The Trackers are operated by distinct third parties: Google LLC (Google
5 Ads / DoubleClick Tracker); Meta Platforms, Inc. (Facebook Pixel Tracker); Microsoft
6 Corporation (Bing / Microsoft Ads Tracker); Klaviyo, Inc. (Klaviyo Tracker); Pinterest,
7 Inc. (Pinterest Tracker); and Criteo S.A. (Criteo Tracker). Defendant enables these
8 trackers, which transmit user data to third-party servers to identify users and support
9 advertising, profiling, and data monetization activities.

10 9. Through the Trackers, the Third Parties collect detailed user information
11 including IP addresses, browser and device type, screen resolution, operating system,
12 pages visited, session duration, scroll depth, mouse movements, click behavior,
13 referring URLs, unique identifiers (such as cookies and ad IDs), and geolocation based
14 on IP. This information is used for behavioral profiling, ad targeting, cross-device
15 tracking, and participation in real-time advertising auctions (collectively, "User
16 Information").

17 10. Because the Trackers capture and transmit users' IP addresses, full page
18 URLs, referrer headers, device identifiers, and other non-content metadata, they
19 function as "pen registers" and/or "trap and trace devices" under Cal. Penal Code §
20 638.50. These tools silently collect routing and addressing information for commercial
21 use without user interaction, as defined in *Greenley v. Kochava, Inc.*, 2023 WL 4833466
22 (S.D. Cal. July 27, 2023).

23 11. Plaintiff and the Class Members did not consent to the installation,
24 execution, embedding, or injection of the Trackers on their devices and did not expect
25 their behavioral data to be disclosed or monetized in this way. By installing and using
26 the Trackers without prior consent and without a court order, Defendant violated CIPA
27 section 638.51.

28 //

1 12. By installing and activating the Trackers without obtaining user consent
2 or a valid court order, Defendant violated California Penal Code § 638.51, which
3 prohibits the use of pen registers and trap and trace devices under these circumstances.

4 13. Defendant provides a privacy policy on the Website (the “Privacy
5 Policy”) but does not conform to the Privacy Policy:

- 6 a. Defendant represents that it engages third-party companies and
7 individuals to help operate, provide, and advertise its services and
8 that such third parties have limited access to personal information
9 and are only permitted to use personal information to perform the
10 identified tasks on Defendant's behalf and are prohibited from
11 disclosing or using personal information for other purposes.
12 Defendant claims limited, purpose-bound sharing, which is
13 inconsistent with the broad dissemination of tracking data to third-
14 party adtech ecosystems with no indication of real-time constraint
15 enforcement.
- 16 b. Defendant does not clearly disclose that real-time behavioral data
17 is transmitted to third parties immediately upon site arrival;
- 18 c. Defendant represents that the Website uses data analytics software
19 to improve its services and that Defendant relies on consumer
20 consent to personalize advertisements on third-party platforms. In
21 reality, the Website provides no initial consent mechanism;
- 22 d. Tracking and third-party sharing occurs prior to presenting users
23 with a valid choice to opt-out or manage consent;

24
25 //

26 //

27 //

28 //

e. Defendant omits material details regarding the depth of personal data shared with third parties and the nature of behavioral profiling activities.

14. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents.

15. Generalized references herein to users, visitors and consumers expressly include Plaintiff and the Class Members.

II. PARTIES

16. Plaintiff MICHAEL HANSON (“Plaintiff”) is a California citizen residing in San Bernardino County and has an intent to remain there. Plaintiff was in California when he visited the Website, which occurred during the class period prior to the filing of the complaint in this matter including but not limited to June 11, 2025, and during which time Plaintiff submitted private information on the Website in order to complete a purchase with a credit card. The allegations set forth herein are based on the Website as configured when Plaintiff visited it.

17. BONANZA WORLDWIDE LLC is a Florida limited liability company that owns, operates and/or controls the Website which is an online platform that offers goods to consumers.

18. BONANZA is an independent online marketplace renowned for its vast selection of unique items and seller-centric approach. The company operates its primary consumer platform at www.bonanza.com and empowers entrepreneurs worldwide to create and grow their businesses without listing fees or monthly store charges.

19. BONANZA is a leading global e-commerce marketplace specializing in one-of-a-kind products, collectibles, and everyday goods. Headquartered in downtown Seattle, Washington, at 3131 Western Avenue, Suite 428, BONANZA offers buyers access to millions of listings from independent sellers across more than 190 countries.

20. The Website serves as the Defendant's flagship consumer-facing brand. As part of its broader commercial ecosystem, BONANZA supports a suite of

1 seller tools such as inventory import from other platforms, customizable marketing
2 campaigns, and automated webstore creation while the Website directly facilitates
3 marketplace transactions, securely processes customer payments, and manages all
4 buyer–seller communications.

5 21. In the course of operating its platform, BONANZA collects and
6 processes significant volumes of user data for transaction fulfillment, behavioral
7 profiling, and targeted advertising, thereby triggering compliance obligations under
8 applicable privacy laws.

9 22. The Website functions as Bonanza’s primary digital storefront, enabling
10 users to explore product listings, save favorites, manage their accounts, and complete
11 purchases. In parallel, BONANZA integrates a variety of third-party tracking
12 technologies, including cookies, advertising pixels, event-tracking scripts, and
13 performance-monitoring tools, to gather granular user interaction data. These practices
14 underpin BONANZA's marketing, audience segmentation, and ad-targeting strategies.

15 **III. JURISDICTION AND VENUE**

16 23. This Court has subject matter jurisdiction over this action pursuant to the
17 Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the total matter in
18 controversy exceeds \$5,000,000 and there are over 100 members of the proposed class.
19 Further, at least one member of the proposed class is a citizen of a State within the
20 United States and at least one defendant is the citizen or subject of a foreign state.

21 24. This Court has personal jurisdiction over Defendant because, on
22 information and belief, Defendant has purposefully directed its activities to the Central
23 District of California by regularly engaging with individuals in California through its
24 Website. Defendant’s illegal conduct is directed at and harms California residents,
25 including Plaintiff, and if not for Defendant’s contact with the forum, Plaintiff would
26 not have suffered harm.

27 25. Venue is proper in the Central District of California pursuant to 28 U.S.C.
28 § 1391 because Defendant (1) is authorized to conduct business in this District and has

intentionally availed itself of the laws and markets within this District; (2) does substantial business within this District; (3) is subject to personal jurisdiction in this District because it has availed itself of the laws and markets within this District; and (4) the injury to Plaintiff occurred within this District.

IV. GENERAL ALLEGATIONS

1. *The California Invasion of Privacy Act (CIPA)*

26. Enacted in 1967, the California Invasion of Privacy Act (CIPA) is a legislative measure designed to safeguard the privacy rights of California residents by prohibiting unauthorized wiretapping and eavesdropping on private communications. The California Legislature recognized the significant threat posed by emerging surveillance technologies, stating that “the development of new devices and techniques for the purpose of eavesdropping upon private communications ... has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society” (Cal. Penal Code § 630).

27. CIPA specifically prohibits the installation or use of “pen registers” and “trap and trace devices” without consent or a court order (Cal. Penal Code § 638.51(a)).

28. A “pen register” is defined as a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, excluding the contents of the communication (Cal. Penal Code § 638.50(b)).

29. Conversely, a “trap and trace device” captures incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, again excluding the contents (Cal. Penal Code § 638.50(b)).

30. In practical terms, a pen register records outgoing dialing information, while a trap and trace device records incoming dialing information.

//

//

1 31. Historically, law enforcement has utilized these devices to monitor
2 telephone calls, with pen registers recording outgoing numbers dialed from a specific
3 line and trap and trace devices recording incoming call numbers to that line.

4 32. Although originally focused on landline telephone calls, CIPA's scope
5 has expanded to encompass various forms of communication, including cell phones and
6 online interactions. For instance, if a user sends an email, a pen register could record
7 the sender's email address, the recipient's email address, and the subject line—
8 essentially capturing the user's outgoing information.

9 33. Similarly, if the user receives an email, a trap and trace device could
10 record the sender's email address, the recipient's email address, and the subject line—
11 capturing the incoming information.

12 34. Despite predating the Internet, CIPA has been interpreted by the
13 California Supreme Court to apply to new technologies where such application does not
14 conflict with the statutory scheme (*In re Google Inc.*, 2013 WL 5423918, at *21;
15 *Greenley*, supra, 2023 WL 4833466, at *15; *Javier v. Assurance IQ, LLC*, 2022 WL
16 1744107, at *1). This interpretation aligns with the principle that CIPA should be
17 construed to provide the greatest privacy protection when faced with multiple possible
18 interpretations (*Matera v. Google Inc.*, 2016 WL 8200619, at *19).

19 35. The conduct alleged herein constitutes a violation of a legally protected
20 privacy interest that is both concrete and particularized. Invasions of privacy have long
21 been actionable under common law. (*Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir.
22 2019); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017).)

23 36. Both the legislative history and statutory language indicate that the
24 California Legislature intended CIPA to protect core privacy rights. Courts have found
25 that violations of CIPA give rise to concrete injuries sufficient to confer standing under
26 Article III. (See *Campbell v. Facebook, Inc.*, 2020 WL 1023350; *In re Facebook*
27 *Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020).)

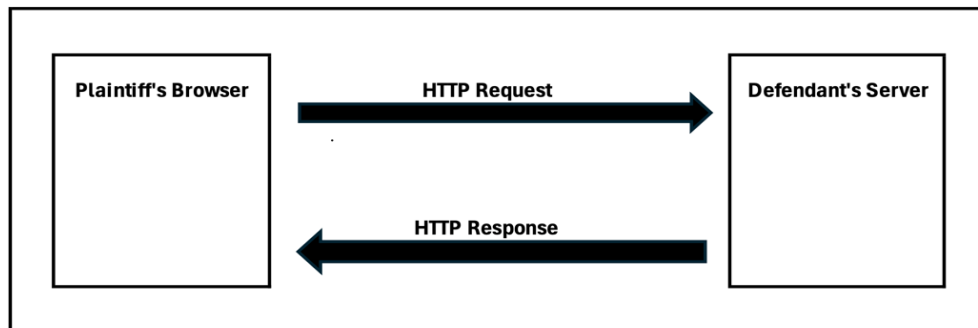
28 //

37. Individuals may pursue legal action against violators of any CIPA provision, including Section 638.51, and are entitled to seek \$5,000 in statutory penalties per violation (Cal. Penal Code § 637.2(a)(1)).

2. The Trackers Are “Pen Registers” and/or “Trap and Trace Devices”

38. When the Plaintiff and Class Members accessed the Website, their browsers initiated an HTTP or HTTPS request to Defendant’s web server, which hosts the content and functionality of the site. In response, the server transmitted an HTTP response containing the necessary resources including HTML, cascading style sheets (CSS), JavaScript files, and image assets used by the browser to render and display the webpage. These resources also included client-side scripts that initiate communication with third-party services for analytics, marketing, and tracking purposes. *Figure 1* below illustrates sample HTTP requests.

Figure 1



39. The server’s response included third-party tracking scripts that were executed by the Plaintiff’s and Class Members’ web browsers. These scripts, once executed, initiate client-side functions that capture routing and behavioral metadata and transmit this data typically via HTTPS requests to the servers of third-party tracking vendors. These actions occur without visible indicators or user awareness. The transmitted data, referred to as User Information, included identifiers such as IP addresses, device characteristics, browser types, page navigation behavior, and unique

1 tracking cookies, all of which were used to profile users and facilitate targeted
2 advertising.

3 40. The Trackers operate by initiating HTTP or HTTPS requests—using
4 either the GET or POST method from the user’s browser to external servers controlled
5 by the Third Parties. These requests are triggered automatically during the page load
6 and by user interactions with the Website. They are used to transmit behavioral data and
7 device metadata, including information such as page views, click events, session
8 duration, and identifying browser characteristics.

9 41. An Internet Protocol (IP) address is a numerical identifier assigned to
10 each device or network connected to the Internet, used to facilitate communication
11 between systems. *See hiQ Labs, Inc. v. LinkedIn Corp.* (9th Cir. 2019) 938 F.3d 985,
12 991 n.4. The most common format, known as IPv4, consists of four numbers separated
13 by periods (e.g., 191.145.132.123). IP addresses enable routing of data between devices
14 and can be used via external geolocation services to infer a user’s general location,
15 including state, city, and in some cases, ZIP code.

16 42. Public IP addresses are unique identifiers assigned by Internet Service
17 Providers (ISPs) that allow devices to communicate directly over the Internet. They are
18 globally accessible, meaning they can be reached from anywhere on the Internet, but
19 are not inherently exposed unless data is being transmitted. Public IP addresses are
20 essential for devices requiring direct Internet access and can be used to approximate a
21 device’s physical location through geolocation services.

22 43. In contrast, private IP addresses are used within internal networks and
23 are not routable on the public Internet. They are isolated from the global Internet and
24 can be reused across different networks without conflict. Unlike public IP addresses,
25 private IP addresses do not divulge a user’s geolocation.

26 44. Public IP addresses play a significant role in digital marketing by
27 enabling geographic targeting based on a user’s approximate location. Through IP
28 geolocation services, advertisers can often determine a user’s country, region, city, and

1 in some cases, ZIP code or service area. In contexts where a static IP address is
2 associated with a fixed residence or business, this data can contribute to household-level
3 or business-level targeting, particularly when combined with other tracking identifiers
4 and third-party enrichment.

5 45. A public IP address functions as “routing, addressing, or signaling
6 information” by facilitating internet communication. It provides essential information
7 that can help determine the general geographic coordinates of a user accessing a website
8 through geolocation databases. Additionally, a public IP address is involved in routing
9 communications from the user’s router to the intended destination, ensuring that emails,
10 websites, streaming content, and other data reach the user correctly.

11 46. As “routing, addressing, or signaling information,” a public IP address is
12 indispensable for maintaining seamless and efficient communication over the Internet.
13 It ensures that data packets are sent from the user’s router to the intended destination,
14 such as a website or email server.

15 47. Defendant installs Trackers on users’ browsers to collect User
16 Information, including IP addresses and full URLs, which constitute outgoing routing
17 and addressing metadata under CIPA. These identifiers serve the same function as
18 telephony dialed numbers and therefore meet the statutory definition of a pen register
19 or trap and trace device.

20 **3. *The Use of Pixel Trackers or Beacons and Digital Fingerprinting***

21 48. Website users typically expect a degree of anonymity when browsing,
22 particularly when they are not logged into an account. However, upon visiting the
23 Website, Plaintiff’s and Class Members’ browsers executed third-party tracking scripts
24 embedded by the Defendant. These Trackers operate in the background of the browsing
25 session and collect detailed behavioral and technical information, which is then
26 transmitted to external third-party servers without the users’ active awareness.

27 49. This process, known as digital fingerprinting, involves compiling various
28 data points such as browser version, screen resolution, installed fonts, device type, and

1 language settings to generate a unique identifier for each user. Fingerprinting can be
2 used to recognize repeat visits and correlate activity across different sessions or sites.
3 When combined with form inputs, login activity, or third-party enrichment,
4 fingerprinting can contribute to broader profiling of a user's interests, affiliations, or
5 behaviors.

6 50. When combined with additional tracking mechanisms such as cookies,
7 login data, and third-party enrichment services, fingerprinting contributes to user
8 profiling. This may include inferring location, browsing habits, consumer preferences,
9 and potentially associating these patterns with known user identities. A sufficiently
10 detailed digital fingerprint, especially when correlated with other identifiers such as
11 email addresses, form submissions, or third-party databases, can enable the
12 reidentification of a user.

13 51. The ability to associate a persistent digital profile with a specific
14 individual using techniques such as digital fingerprinting has led to the development of
15 a data industry known as identity resolution. Identity resolution involves recognizing
16 users across sessions, devices, and platforms by connecting various identifiers derived
17 from their digital behavior, including IP addresses, browser metadata, cookies, and, in
18 some cases, login credentials. The process may occur deterministically (based on
19 known logins or user-submitted information) or probabilistically (based on behavioral
20 or technical similarity).

21 52. In simpler terms, pen register and trap and trace mechanisms in the digital
22 context refer to technologies that record metadata such as IP addresses, URLs visited,
23 and device characteristics, information that identifies the routing and addressing of
24 electronic communications. This can be achieved through the deployment of tracking
25 technologies like the Trackers installed, executed, embedded or injected in the Website,
26 which operate without user interaction or visibility.

27 53. The Trackers provide analytics and marketing services to Defendant
28 using the data collected from visitors to the Website. These services also leverage user

1 data collected from other websites that include the same pen register and trap and trace
2 devices operated by the Third Parties.

3 54. When users visit the Website, installed, executed, embedded or injected
4 Trackers initiate network requests to third-party servers, using invisible image pixels,
5 JavaScript calls, or beacon APIs. These requests include the user's IP address, which is
6 transmitted automatically as part of the HTTP request header. In many cases, the
7 Tracker's server responds by placing a persistent cookie in the user's browser, which
8 serves as a unique identifier that can be used to recognize and track the user across
9 future visits. If a user deletes their browser cookies, this identifier is removed.
10 However, upon revisiting the Website, the process repeats: the browser executes the
11 Tracker's script, a new identifier is set, and the Tracker resumes collecting the user's IP
12 address and associated behavioral data.

13 4. *Plaintiff's And Class Members' Data Has Financial Value*

14 55. Given the number of Internet users, the "world's most valuable resource
15 is no longer oil, but data."¹

16 56. Consumers' web browsing histories have an economic value more than
17 \$52 per year, while their contact information is worth at least \$4.20 per year, and their
18 demographic information is worth at least \$3.00 per year.²

19 57. There is "a study that values users' browsing histories at \$52 per year, as
20 well as research panels that pay participants for access to their browsing histories."³

21 58. Extracted personal data can be used to design products, platforms, and
22 marketing techniques. A study by the McKinsey global consultancy concluded that
23

24 ¹ Ian Cohen, Are Web-Tracking Tools Putting Your Company at Risk?, Forbes (Oct
25 19, 2022), <https://www.forbes.com/sites/forbestechcouncil/2022/10/19/are-web-tracking-tools-putting-your-company-atrisk/?sh=26481de07444>

26 ² *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 928 (N.D. Cal.
27 2015), rev'd, 956 F.3d 589 (9th Cir. 2020).

28 ³ *In re Facebook, Inc. Internet Tracking Litigation* (9th Cir. 2020) 956 F.3d 589, 600.

1 businesses that “leverage customer behavior insights outperform peers by 85 percent in
2 sales growth and more than 25 percent in gross margin.”⁴

3 59. In 2013, the Organization for Economic Cooperation and Development
4 (“OECD”) estimated that data trafficking markets had begun pricing personal data,
5 including those obtained in illicit ways without personal consent. It found that illegal
6 markets in personal data valued each credit cardholder record at between 1 and 30 U.S.
7 dollars in 2009, while bank account records were valued at up to 850 U.S. dollars. Data
8 brokers sell customer profiles of the sort that an online retailer might collect and
9 maintain for about 55 U.S. dollars, and that individual points of personal data ranged in
10 price from \$0.50 cents for an address, \$2 for a birthday, \$8 for a social security number,
11 \$3 for a driver’s license number, and \$35 for a military record (which includes a birth
12 date, an identification number, a career assignment, height, weight, and other
13 information). Experiments asking individuals in the United States and elsewhere how
14 much they value their personal data points result in estimates of up to \$6 for purchasing
15 activity, and \$150-240 per credit card number or social security number.⁵

16 60. The last estimate probably reflects public reporting that identify theft
17 affecting a credit card number or social security number can result in financial losses of
18 up to \$10,200 per victim.⁶

19 61. The Defendant’s monetization of personal data constitutes actionable
20 economic harm under federal law, even without evidence of a direct financial loss, as a

21 ⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto,
22 Capturing value from your customer data, McKinsey (Mar. 15, 2017),
23 [https://www.mckinsey.com/businessfunctions/quantumblack/ourinsights/capturing-](https://www.mckinsey.com/businessfunctions/quantumblack/ourinsights/capturing-value-from-your-customer-data)
24 [value-from-your-customer-data](https://www.mckinsey.com/businessfunctions/quantumblack/ourinsights/capturing-value-from-your-customer-data)

25 ⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for
26 Measuring Monetary Value, OECD Digital Economy Papers, No. 220 (Apr. 2,
2013), at 27-28, <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>

27 ⁶ Bradley J. Fikes, Identity Theft Hits Millions, Report Says, San Diego Union
28 Tribune, Sept. 4, 2003, [https://www.sandiegouniontribune.com/sdut-identity-theft-](https://www.sandiegouniontribune.com/sdut-identity-theft-hits-millions-report-says-2003sep04-story.html)
[hits-millions-report-says-2003sep04-story.html](https://www.sandiegouniontribune.com/sdut-identity-theft-hits-millions-report-says-2003sep04-story.html).

1 “misappropriation-like injury” caused by converting user data into a revenue stream
2 through targeted advertising. *In re Facebook, Inc. Internet Tracking Litigation*, 956
3 F.3d 589 (9th Cir. 2020).

4 **5. Defendant Is Motivated To Monetize Consumer Information**
5 ***Regardless of Consent***

6 62. Data harvesting is one of the fastest growing industries in the country,
7 with estimates suggesting that internet companies earned \$202 per American user in
8 2018 from mining and selling data. That figure is expected to increase with estimates
9 for 2022 as high as \$434 per use, reflecting a more than \$200 billion industry.

10 63. By implementing Trackers on the Website, Defendant participates in
11 building detailed behavioral profiles of visitors. These profiles may include information
12 such as which users viewed specific products, engaged with pages or interface elements,
13 or demonstrated purchase intent. This data enables Defendant and its advertising
14 partners to identify repeat visits from the same device or browser. The behavioral data
15 is integrated into third-party advertising platforms, allowing Defendant to deliver
16 retargeted ads to users who previously visited the Website, offer promotional incentives
17 to re-engage high-intent visitors, and build “lookalike audiences” that target users with
18 similar behaviors or characteristics. These practices significantly improve advertising
19 efficiency and increase the likelihood of converting user engagement into actual sales.

20 64. Defendant has a strong financial incentive to deploy the Trackers on its
21 Website without obtaining user consent. By enabling the collection of IP addresses and
22 device-level identifiers through these technologies, Defendant facilitates integration
23 into real-time bidding ecosystems. These systems rely on bidstream data such as IP
24 address, device type, screen resolution, and referral information to assess the value of a
25 potential ad impression. This enables Defendant and its partners to participate in data-
26 driven ad targeting, increase the value of its advertising inventory, and track users across
27 sessions and websites, all of which provide economic benefit despite private
28 implications to users.

65. IP addresses are a valuable data point in digital advertising and tracking systems. They can be used to approximate a user's geographic location, often down to the city or ZIP code level, enabling location-based targeting. When combined with cookies, browser metadata, and device identifiers, IP addresses contribute to persistent user tracking across sessions and websites. They also assist advertisers and data brokers in linking anonymous browsing activity to existing user profiles, which enhances ad targeting precision and increases the commercial value of each tracked interaction. IP addresses therefore constitute "routing, addressing, or signaling information" protected under CIPA § 638.50(b).

66. When users' data is collected without meaningful consent and monetized, they lose control over who can access, use, or distribute their personal information. Data brokers and ad tech firms aggregate and correlate identifiers such as IP addresses, device IDs, and cookies with other personal data to construct detailed consumer profiles. Information initially gathered in one context, such as browsing a retail website, is frequently repurposed for unrelated uses and sold to third parties without the user's awareness. This results in pervasive surveillance, where users are continuously tracked across multiple websites, applications, and devices, often without their knowledge or ability to opt out.

6. *The Trackers Function Together to Achieve Targeted Objectives*

67. When a visitor arrives on the Website, a coordinated suite of background tracking technologies activates instantly upon page load. These include client-side scripts deployed by Google Ads/DoubleClick, Facebook Pixel, Bing/Microsoft Ads, Klaviyo, Pinterest, and Criteo, each silently collecting categories of user information such as browsing behavior, device details, and referral data without any visible notification. Working in concert, these trackers form an integrated data-collection infrastructure that empowers Defendant to analyze user actions at a granular level and leverage those insights in real time for marketing optimization, personalized targeting, and strategic business intelligence.

68. On page load, third-party tracking scripts for Google Ads/DoubleClick, Facebook Pixel, Bing/Microsoft Ads, Klaviyo, Pinterest, and Criteo are fetched and executed in the background. Each script begins gathering user-specific data, ranging from cookie identifiers and click events to form interactions and time-on-page metrics, without any explicit user prompt or banner. Collectively, these trackers deliver a synchronized data stream that enables real-time decisioning across Defendant's advertising and analytics systems. The Trackers do not operate in isolation but as nodes within a vast, interconnected digital-advertising ecosystem. Through shared identifiers, cookie syncing, and cross-device techniques, the Trackers continually exchange and match user identifiers. This networked approach builds persistent consumer profiles, enhancing identity resolution, behavioral targeting, and user segmentation at scale in real time.

69. Defendant embeds Google Ads/DoubleClick, Facebook Pixel, Bing/Microsoft Ads, Pinterest, and Criteo trackers directly in the initial HTML markup, causing them to fire immediately upon load. Klaviyo's tracking scripts are similarly embedded for email-related engagement, while additional Klaviyo and Pinterest trackers may be injected dynamically via JavaScript functions during page rendering. All the Trackers operate in tandem to capture and relay user interaction data such as page views, add-to-cart events, and checkout progress, enabling downstream ad targeting, profiling, and data-sharing processes.

70. Identity resolution leverages the combined capabilities of Facebook Pixel, Klaviyo, and Pinterest. Facebook Pixel links on-site behavior to logged-in Facebook sessions and cookie histories, matching browsing actions to social identities. Klaviyo Tracker captures email addresses, purchase events, and custom properties to tie online behavior back to individual subscribers. Pinterest Tracker uses tag firing and cookie data to connect site interactions with Pinterest user profiles. Together, these tools enable Defendant to de-anonymize visitors over time, aligning behavioral signals with known identities and enriching demographic and interest profiles.

1 71. Once identity signals are collected, targeted ad delivery and data
2 monetization occur through Google Ads/DoubleClick, Criteo, and Bing/Microsoft Ads.
3 Google Ads/DoubleClick participates in real-time bidding (RTB), using conversion
4 history and audience data to serve performance-optimized creatives. Criteo's
5 retargeting engine ingests browsing events and purchase intent signals to personalize
6 display ads across its network. Bing/Microsoft Ads leverages event-level data to
7 remarket visitors on Microsoft's properties and partner sites. These trackers transform
8 user interactions into monetizable audience segments, driving measurable advertising
9 outcomes for Defendant.

10 72. Defendant's tracking infrastructure transmits user data to third-party ad
11 platforms such as Google Ads/DoubleClick, Facebook Pixel, Bing/Microsoft Ads,
12 Klaviyo, Pinterest, and Criteo immediately upon page load, before any opt-in or consent
13 mechanism is presented. Collected identifiers include IP addresses, browser and device
14 characteristics, referral URLs, and cookie values. This silent data flow enables
15 advertisers to continuously track visitors across sessions and websites, building
16 persistent profiles and serving personalized ads in real time.

17 73. Network requests to Google Ads/DoubleClick, Criteo, and
18 Bing/Microsoft Ads conversion and bidding endpoints demonstrate Defendant's
19 integration into programmatic advertising architectures. When a user lands on the site,
20 trackers issue silent bid requests containing user identifiers and behavioral signals to
21 RTB exchanges. Advertisers then bid on impressions based on those signals, allowing
22 Defendant to monetize user attention by selling access to targeted audiences. These
23 processes serve purely commercial objectives, treating personal data as a revenue-
24 generating commodity rather than a functional necessity for the user.

25
26 //

27 //

28 //

V. SPECIFIC ALLEGATIONS

1. *Google Ads / DoubleClick Tracker*

74. The Google Ads / DoubleClick Tracker is a digital advertising, behavioral tracking, and data brokering technology operated by Google LLC. It is designed to deliver display advertisements, measure engagement, and support real-time bidding on programmatic ad exchanges. The Google Ads / DoubleClick Tracker enables Google and its advertising clients to collect detailed user interaction data and optimize ad delivery across a vast network of third-party websites.

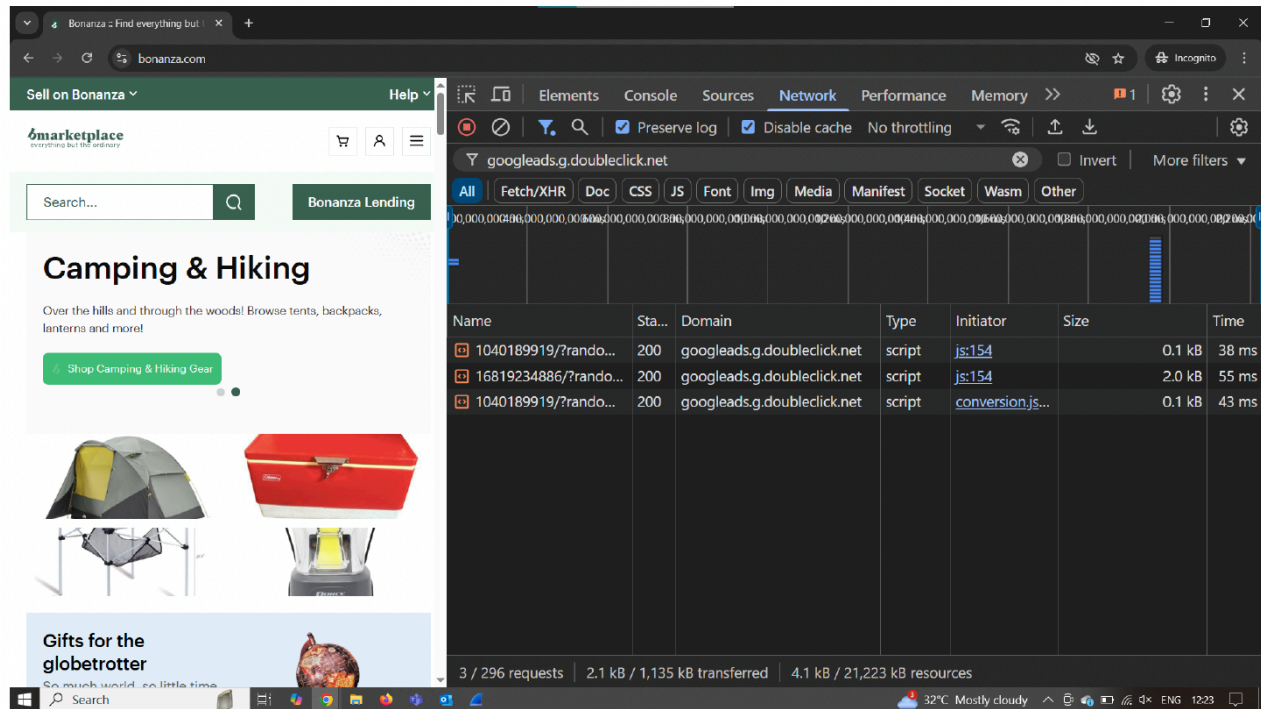
75. When implemented on the Website, the Google Ads Tracker collects a broad set of user metadata, including visited URLs, session timestamps, referrer headers, and in-page activity data such as page views and navigation events. It also captures technical device attributes such as IP address, screen resolution, browser type, operating system, and language settings. These data points are linked to persistent browser identifiers placed via cookies or pixel fires that allow Google to track users across multiple websites, sessions, and devices, forming longitudinal behavioral profiles. The Google Ads Tracker also transmits conversion tracking signals and remarketing data, enabling Google to associate Website interactions with ad conversion events and to retarget users across its advertising ecosystem.

76. The Google Ads Tracker facilitates monitoring of user activity on the Website, including the capture of pageview events and other engagement signals that can be used to track user progression through various transactional flows. These interaction signals are transmitted to Google's ad infrastructure to facilitate targeted advertising, audience retargeting, and conversion tracking. The Google Ads Tracker executes via JavaScript calls to domains including `googleads.g.doubleclick.net` and activates automatically upon page load without requiring any action by the user.

77. *Figure 2* below is a screenshot from the Website, confirming that the Google Ads was triggered automatically upon visiting the homepage. *Figure 2* captures a network request from the Website to `googleads.g.doubleclick.net` within milliseconds

of page load. This domain is part of Google's advertising infrastructure and is used to log ad impressions, behavioral signals, referrer data, and user device information. This request occurs without any indication to the user that Google Ads infrastructure has been activated and without the user being provided any choice or control.

Figure 2



78. **Figure 3** below captures a POST request from the Website to analytics.google.com. The presence of this POST request within seconds of page load confirms that Google Analytics has been activated as part of the initial load sequence, before user interaction. Though the interaction is invisible to the visitor, it means that Google begins learning about their behavior immediately and without any opportunity to obtain consent.

//

//

//

//

Figure 3

Source	Destination	Protocol	Length	Info
198.19.190.52	198.19.0.2	DNS	80	Standard query 0x24cb A fonts.googleapis.com
198.19.0.2	198.19.190.52	DNS	96	Standard query response 0x24cb A fonts.googleapis.com A 142.2...
198.19.190.52	198.19.0.2	DNS	84	Standard query 0x077f A www.google-analytics.com
198.19.0.2	198.19.190.52	DNS	180	Standard query response 0x077f A www.google-analytics.com A 1...
198.19.190.52	198.19.0.2	DNS	84	Standard query 0x6479 A www.googleadservices.com
198.19.0.2	198.19.190.52	DNS	116	Standard query response 0x6479 A www.googleadservices.com A 1...
198.19.190.52	198.19.0.2	DNS	74	Standard query 0x0051 A www.google.com
198.19.0.2	198.19.190.52	DNS	170	Standard query response 0x0051 A www.google.com A 142.251.111...
198.19.190.52	198.19.0.2	DNS	87	Standard query 0xab01 A googleads.g.doubleclick.net
198.19.0.2	198.19.190.52	DNS	119	Standard query response 0xab01 A googleads.g.doubleclick.net ...
198.19.190.52	198.19.0.2	DNS	80	Standard query 0xc909 A analytics.google.com
198.19.0.2	198.19.190.52	DNS	172	Standard query response 0xc909 A analytics.google.com CNAME a...
198.19.190.52	198.19.0.2	DNS	91	Standard query 0x5c69 A content-autofill.googleapis.com
198.19.0.2	198.19.190.52	DNS	283	Standard query response 0x5c69 A content-autofill.googleapis...
198.19.190.52	198.19.0.2	DNS	70	Standard query 0x72f8 A google.com
198.19.0.2	198.19.190.52	DNS	166	Standard query response 0x72f8 A google.com A 142.250.31.139 ...

Frame 3055: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{4DCE21C...}

Ethernet II, Src: 0e:78:b2:33:3b:ef (0e:78:b2:33:3b:ef), Dst: 0e:f7:cf:91:4c:ff (0e:f7:cf:91:4c:ff)

79. Defendant surreptitiously installed, executed, embedded or injected the Google Ads / DoubleClick Tracker onto users' browsers by embedding tracking scripts in the Website's page source and by dynamically injecting additional JavaScript tracking code during runtime. When a user visits the Website, their browser automatically executes this code, which initiates outbound network requests to Google's advertising servers and transmits metadata including IP address, page URL, referrer information, device details, behavioral identifiers, and conversion tracking parameters as part of a third-party ad targeting, profiling, and data brokering system.

80. The Google Ads / DoubleClick Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

81. The Google Ads / DoubleClick Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. *See, e.g., James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

82. The Google Ads / DoubleClick Tracker functions as a pen register and/or trap and trace device under the California Invasion of Privacy Act because it captures

1 outgoing signaling data such as URLs visited, timestamps, and referrer headers and also
2 processes incoming metadata such as ad impressions and cookie-based session
3 identifiers. These transmissions occur automatically during page load and without user
4 participation, enabling Google to continuously log user behavior and associate it with
5 broader advertising profiles.

6 83. Defendant never obtained a court order permitting the installation of a
7 pen register or trap and trace device or process and did not obtain Plaintiff's or the Class
8 Members' express or implied consent to install the Google Ads / DoubleClick Tracker
9 on Plaintiff's and Class Members' browser or to collect or share data with Google.

10 84. Consequently, the Google Ads / DoubleClick Tracker violates CIPA
11 regarding unauthorized use of a pen register and/or trap and trace device without prior
12 consent or court order.

13 **2. *The Facebook Pixel Tracker***

14 85. The Facebook Pixel Tracker is a behavioral tracking script implemented
15 through Meta's Pixel technology, and in this case, it is delivered from the
16 domain connect.facebook.net. On the Website, the Facebook Pixel Tracker is injected
17 using client-side scripting methods, likely managed through a tag management system
18 or direct implementation within the source code. Once the script is initialized, it begins
19 background communication with Meta's servers, enabling real-time monitoring of user
20 activity across the Website.

21 86. When a user visits the homepage of the Website, the Facebook Pixel
22 Tracker activates automatically during page load and immediately begins collecting
23 behavioral data. This includes the logging of standard interaction signals such as page
24 views, time spent on page, and general navigation activity. The script passively detects
25 and records user engagement signals such as mouse movements, clicks, and scrolling
26 behavior. These data signals are sent to Meta's infrastructure, where they may be
27 associated with the user's Facebook or Instagram account, regardless of whether the
28 user directly interacts with any Meta service while on the Website.

1 87. The data gathered by the Facebook Pixel Tracker facilitates identity
2 resolution by linking behavioral activity observed on the Website with individual Meta
3 user profiles. If the visitor is signed into Facebook, Instagram, or Messenger on the
4 same device or browser, the script is capable of connecting Website behavior to that
5 individual's Meta ID. In cases where the user is not logged into a Meta platform, a
6 persistent identifier may still be assigned using browser fingerprinting techniques or
7 through cookie storage and pixel data. This process supports the development of
8 detailed behavioral profiles across browsing sessions and platforms.

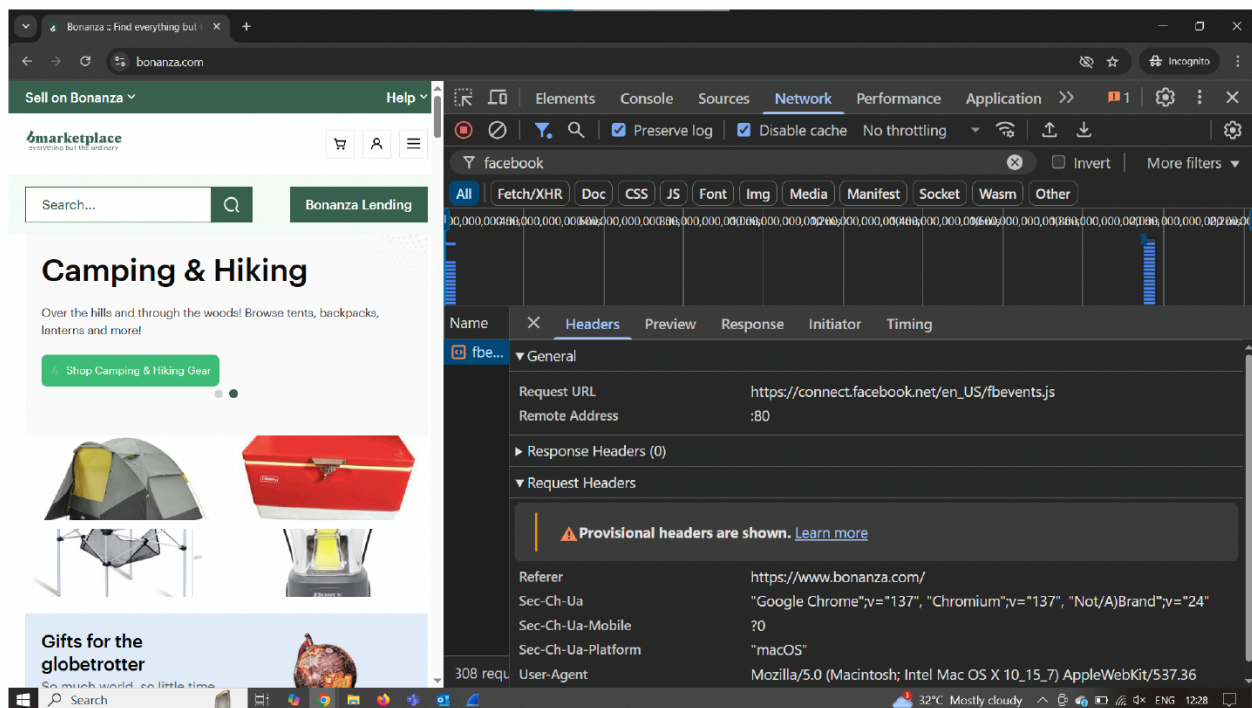
9 88. The Facebook Pixel Tracker also supports the Website's marketing and
10 advertising efforts by enabling Meta's "Custom Audiences" functionality. This feature
11 allows the Website to build segmented groups of users who have engaged in specific
12 activities, such as viewing products or initiating a checkout. These audiences can then
13 be re-targeted through Meta's advertising networks, including Facebook and Instagram.
14 Additionally, the Website can generate "Lookalike Audiences," which consist of new
15 users who share behavioral traits with the original audience segments, thereby
16 expanding advertising reach and effectiveness.

17 89. The Facebook Pixel Tracker contributes to the Website's advertising
18 performance strategy by transforming user behavior data into actionable insights. Real-
19 time analytics are generated concerning user interaction, advertising campaign success,
20 and conversion performance. These metrics are reported back through Meta's
21 advertising tools, allowing the Website to optimize advertising spend, tailor marketing
22 messages, and enhance return on investment. As a result, the Facebook Pixel Tracker
23 functions as a foundational element in the Website's behavioral analytics and targeted
24 advertising infrastructure.

25 90. **Figure 4** below is a screenshot from the Website, confirming that the
26 Facebook Pixel infrastructure was activated during the user's session on the
27 homepage. A request to connect.facebook.net was initiated automatically as part of the
28 initial page load sequence, prior to any user interaction or opportunity to provide

informed consent. Specifically, the request targeted the file fbevents.js, which is the core script powering Facebook Pixel tracking capabilities. This JavaScript resource enables Facebook to collect detailed behavioral data including page views, session metadata, referrer URLs, and device information. The request returned a successful response (HTTP 200), indicating active communication with Meta's servers without the presentation of any visible cookie banner, opt-in mechanism, or privacy warning at the time of execution.

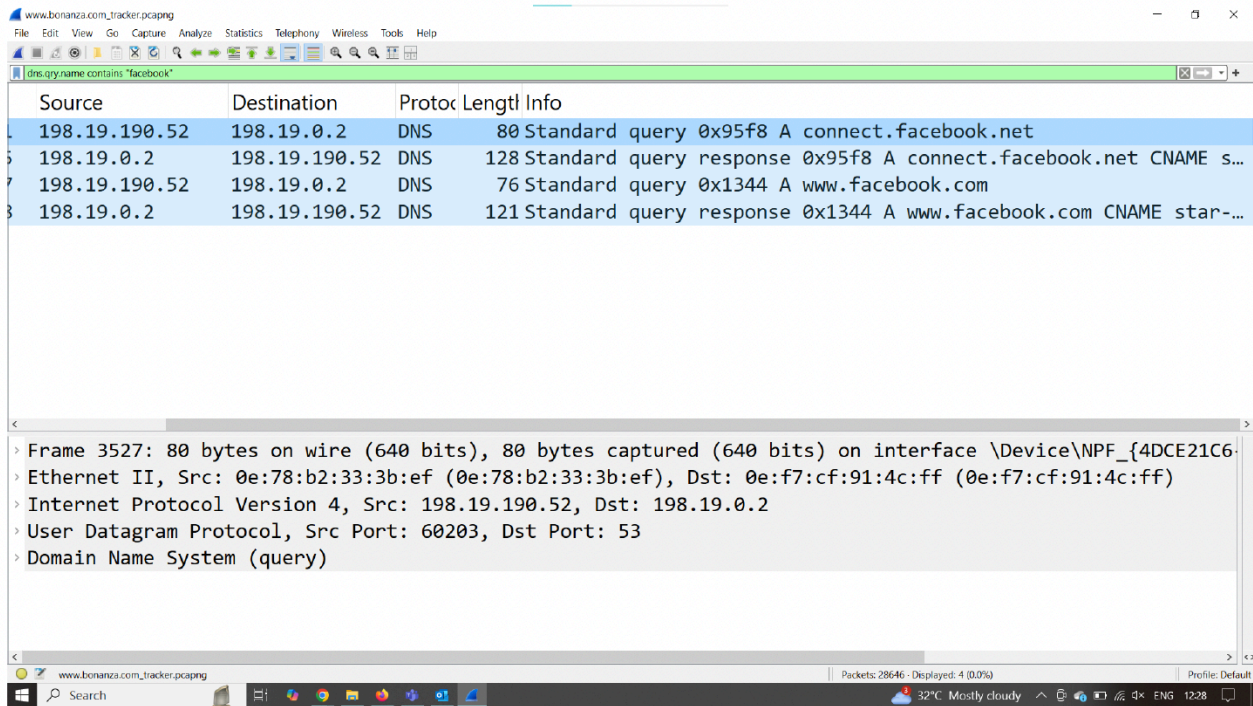
Figure 4



91. **Figure 5** below is a screenshot of network-level activity confirming that Bonanza.com initiated communication with Meta's infrastructure during the initial moments of a user's session. Specifically, a DNS query was issued for the domain connect.facebook.net, and a corresponding DNS resolution was completed by the visitor's device within seconds of arriving on the homepage. This type of background DNS resolution occurs automatically, without any user interaction or awareness, and serves as definitive evidence that the browser was instructed to prepare a connection to Meta's servers. Even in the absence of cookies or visible tracking

scripts, the DNS query itself demonstrates that the Website silently began establishing communication pathways with Facebook, as DNS queries are part of the broader act of interception. This screenshot illustrates that Meta’s tracking systems are engaged behind the scenes as soon as a visitor lands on the Website without notice, opt-out options, or informed consent.

Figure 5



Source	Destination	Protocol	Length	Info
198.19.190.52	198.19.0.2	DNS	80	Standard query 0x95f8 A connect.facebook.net
198.19.0.2	198.19.190.52	DNS	128	Standard query response 0x95f8 A connect.facebook.net CNAME s...
198.19.190.52	198.19.0.2	DNS	76	Standard query 0x1344 A www.facebook.com
198.19.0.2	198.19.190.52	DNS	121	Standard query response 0x1344 A www.facebook.com CNAME star...

Frame 3527: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{4DCE21C6...}

Ethernet II, Src: 0e:78:b2:33:3b:ef (0e:78:b2:33:3b:ef), Dst: 0e:f7:cf:91:4c:ff (0e:f7:cf:91:4c:ff)

Internet Protocol Version 4, Src: 198.19.190.52, Dst: 198.19.0.2

User Datagram Protocol, Src Port: 60203, Dst Port: 53

Domain Name System (query)

92. Defendant surreptitiously installed, executed, embedded, or injected the Facebook Pixel Tracker onto users’ browsers by dynamically injecting Meta’s JavaScript pixel through a tag management system such as Google Tag Manager. When a user visits the Website, the browser automatically executes this script, triggering outbound requests to Meta’s servers and transmitting metadata including the user’s page URL, referrer, browser configuration, and other session-specific details. These tracking operations occur without any user interaction, allowing Meta to collect data from users’ sessions silently and without their consent.

93. The Facebook Pixel Tracker is at least a “process” because it is software that identifies consumers, gathers data, and correlates that data.

1 94. The Facebook Pixel Tracker is at least a “device” because in order for
2 software to work, it must be run on some kind of computing device. See, e.g., *James v.*
3 *Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

4 95. The Facebook Pixel Tracker captures and transmits routing, addressing,
5 and signaling information such as the user’s page URL, referrer, and browser metadata
6 to Meta’s servers as soon as the page loads, without the user’s knowledge or consent.
7 This type of metadata reveals the origin and destination of the user’s electronic
8 communications. The connection is not initiated by the user, but rather by code
9 embedded in the Website, allowing Meta to intercept and associate those signals with a
10 known or inferred identity. The transmission occurs while the user’s communication is
11 still in transit and is diverted to Meta without authorization.

12 96. Defendant never obtained a court order permitting the installation of a
13 pen register or trap and trace device or process and did not obtain Plaintiff’s or the Class
14 Members’ express or implied consent to install the Facebook Pixel Tracker on
15 Plaintiff’s and Class Members’ browser or to collect or share data with Facebook.

16 97. Consequently, the Facebook Pixel Tracker violates CIPA regarding
17 unauthorized use of a pen register and/or trap and trace device without prior consent or
18 court order.

19 **3. The Bing / Microsoft Ads Tracker**

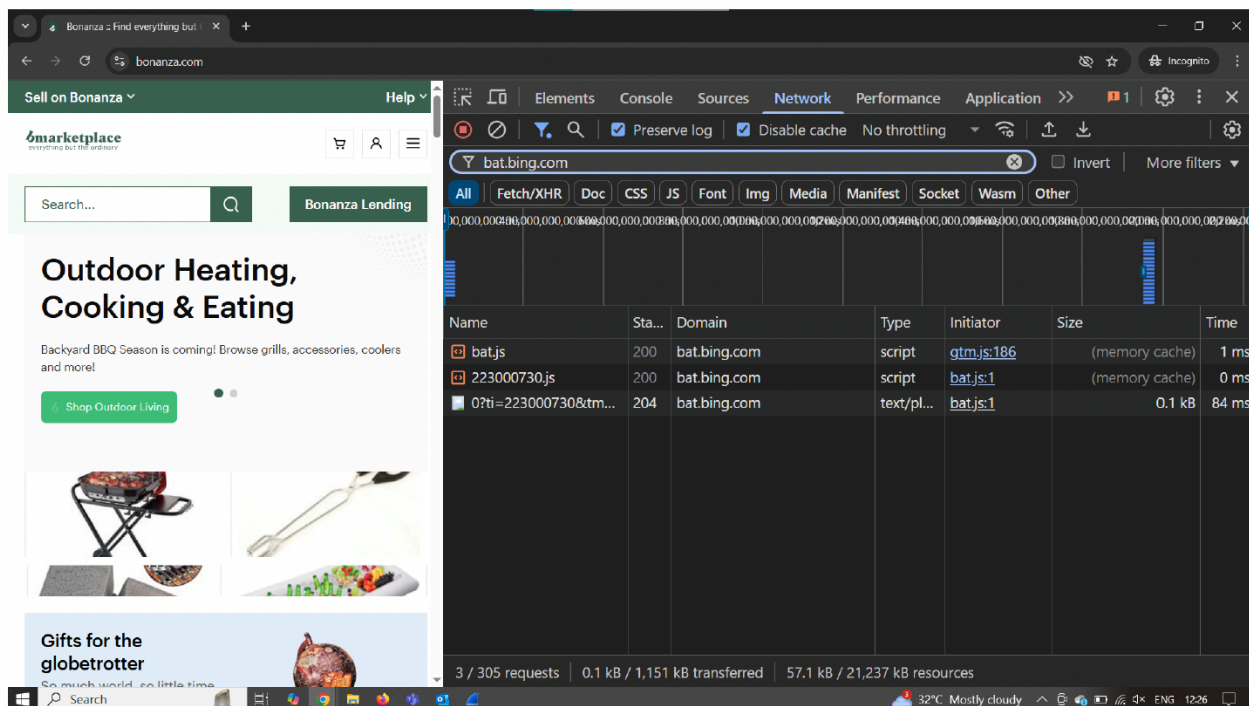
20 98. The Bing / Microsoft Ads Tracker, typically delivered through the
21 domain bat.bing.com, is part of the Microsoft Advertising platform (formerly Bing
22 Ads). It is used to track user interactions on websites in order to attribute conversions,
23 retarget visitors, and optimize advertising campaigns across Microsoft’s search and
24 display networks, including Bing, MSN, and LinkedIn.

25 99. The Bing / Microsoft Ads Tracker is designed to silently collect a range
26 of user data when a visitor lands on the Website. It gathers device and browser metadata,
27 IP address, estimated geolocation, referrer URLs, and viewed pages. It is also designed
28 to capture click events and conversion actions, such as form submissions or account

sign-ups on the Website. Through the use of cookies and unique identifiers, the Bing / Microsoft Ads Tracker can track users across sessions and websites to build behavioral profiles and deliver targeted advertising.

100. **Figure 6** below is a screenshot from the Website, confirming that Microsoft's Bing Ads tracking script was activated during the user's session on the homepage. A request to <https://bat.bing.com/bat.js> was captured as part of the core load sequence for the Website, occurring automatically upon page load and without any user interaction. This file, bat.js, is Microsoft's Behavioral Analytics Tracker, which enables Bing Ads to collect extensive telemetry on the visitor, including device and browser details, IP address, referrer information, and user engagement metrics. The presence and execution of this script indicate that Microsoft's advertising and tracking infrastructure is engaged silently in the background from the moment the page loads without presenting the user with any visible consent banner or opt-in mechanism.

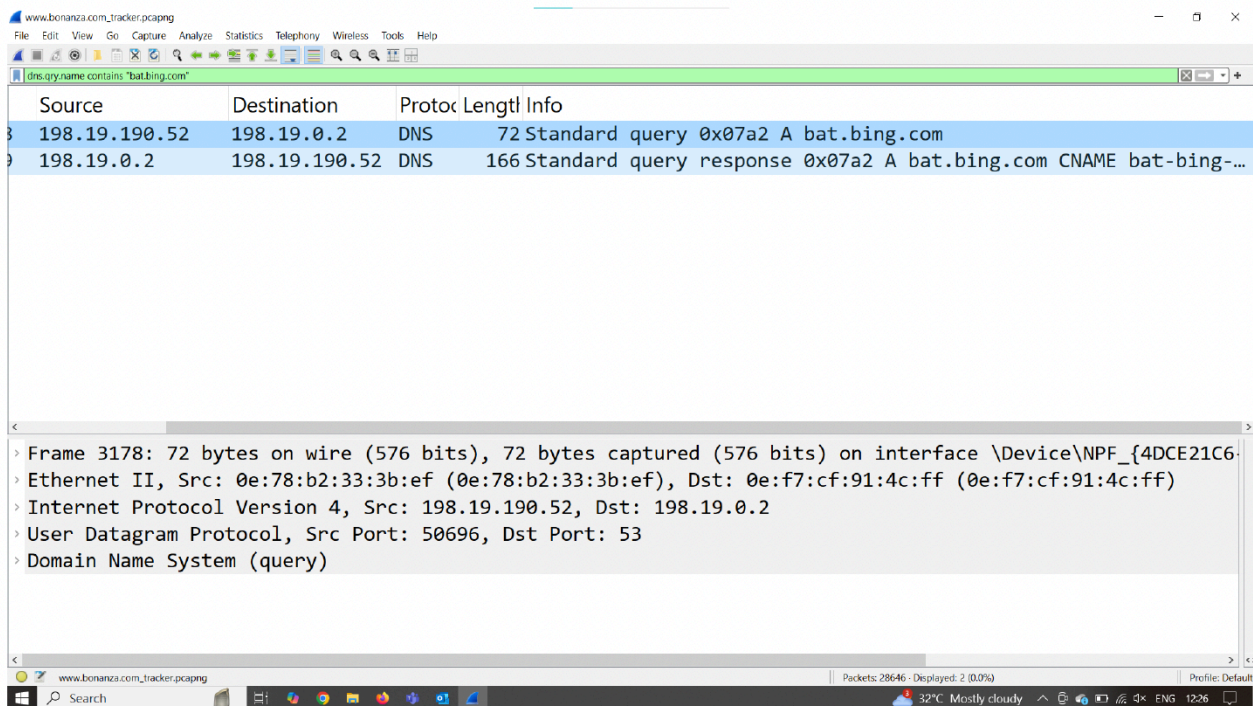
Figure 6



101. **Figure 7** below is a screenshot of backend network activity confirming that Bonanza.com initiated communication with Microsoft Bing Ads infrastructure

during the initial moments of a user's visit. A DNS query for the domain bat.bing.com was issued by the user's device within seconds of the homepage loading. This resolution occurred automatically, before the visitor had a chance to scroll, click, or interact in any way, indicating that the browser was instructed to prepare a connection to Microsoft's advertising servers immediately upon arrival. Although no visual elements or alerts were presented to the user, the DNS query itself demonstrates that tracking infrastructure was activated in the background.

Figure 7



102. Defendant surreptitiously installed, executed, and embedded the Bing / Microsoft Ads Tracker onto users' browsers by including Microsoft's JavaScript tracking code directly in the Website's source code. When a user visits the Website, their browser executes this code, which triggers outbound requests to Microsoft's servers and transmits metadata including the user's IP address, page URL, referrer, and session-specific identifiers.

103. The Bing / Microsoft Ads Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

104. The Bing / Microsoft Ads Tracker is at least a “device” because in order for software to work, it must be run on some kind of computing device. See, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

105. The Bing / Microsoft Ads Tracker initiates a connection to its ad infrastructure upon page load via a script or pixel execution. It captures user metadata such as IP address, page path, timestamp, and unique identifiers - all of which qualify as routing or signaling information under CIPA.

106. The Bing / Microsoft Ads Tracker collects real-time signaling and routing information from the user’s device without direct interaction. It acts as a pen register by capturing outbound metadata such as page visits, click events, and form submissions, and as a trap and trace device by receiving inbound responses like ad content and tracking pixels. These communications occur passively, enabling Microsoft to assign user identifiers, build behavior profiles, and facilitate personalized advertising, all without the user’s knowledge or consent.

107. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff’s or the Class Members’ express or implied consent to install the Bing / Microsoft Ads Tracker on Plaintiff’s and Class Members’ browser or to collect or share data with Microsoft.

108. Consequently, the Bing / Microsoft Ads Tracker violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

VI. CLASS ALLEGATIONS

109. Plaintiff brings this action individually and on behalf of all others similarly situated (the “Class” or “Class Members”) defined as follows:

All persons within California whose browser was subject to installation, execution, embedding, or injection of the Trackers by the Defendant’s Website during the relevant statute of limitations period.

1 **110. NUMEROSITY:** Plaintiff does not know the number of Class Members
 2 but believes the number to be in the thousands, if not more. The exact identities of
 3 Class Members can be ascertained by the records maintained by Defendant.

4 **111. COMMONALITY:** Common questions of fact and law exist as to all
 5 Class Members and predominate over any questions affecting only individual members
 6 of the Class. Such common legal and factual questions, which do not vary between
 7 Class members, and which may be determined without reference to the individual
 8 circumstances of any Class Member, include but are not limited to the following:

- 9 • Whether Defendant installed, executed, embedded or injected the Trackers
 10 on the Website;
- 11 • Whether the Trackers are each a pen register and/or trap and trace device as
 12 defined by law;
- 13 • Whether Plaintiff and Class Members are subject to same tracking policies
 14 and practices;
- 15 • Whether Plaintiff and Class Members are entitled to statutory damages;
- 16 • Whether Class Members are entitled to injunctive relief;
- 17 • Whether Class Members are entitled to disgorgement of data unlawfully
 18 obtained;
- 19 • Whether the Defendant's conduct violates CIPA; and
- 20 • Whether the Defendant's conduct constitutes an unlawful, misleading,
 21 deceptive or fraudulent business practice.

22 **112. TYPICALITY:** As a person who visited Defendant's Website and
 23 whose outgoing electronic information was surreptitiously collected by the Trackers,
 24 Plaintiff is asserting claims that are typical of the Class Members. Plaintiff's experience
 25 with the Trackers is typical to Class Members.

26 **113. ADEQUACY:** Plaintiff will fairly and adequately protect the interests
 27 of the members of the Class. Plaintiff has retained attorneys experienced in class action
 28

litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the Class or whose inclusion would otherwise be improper are excluded.

114. **SUPERIORITY:** A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class Members is impracticable and inefficient. Even if every Class Member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

VII. FIRST CAUSE OF ACTION

Violations of Cal. Penal Code § 638.51

By Plaintiff and the Class Members Against All Defendants

115. Plaintiff reasserts and incorporates by reference the allegations set forth in each preceding paragraph as though fully set forth herein.

116. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

117. Defendant uses a pen register device or process and/or a trap and trace device or process on its Website by deploying the Trackers because the Trackers are designed to capture the IP address, User Information and other information such as the phone number, email, routing, addressing and/or other signaling information of website visitors.

118. Defendant did not obtain consent from Plaintiff or any of the Class Members before using pen registers or trap and trace devices to locate or identify users of its Website and has thus violated CIPA. CIPA imposes civil liability and statutory penalties for violations of § 638.51. Cal. Penal Code § 637.2; *Moody v. C2 Educational Systems, Inc.*, No. 2:24-cv-04249-RGK-SK, 2024 U.S. Dist. LEXIS 132614 (C.D. Cal. July 25, 2024).

//

//

VIII. SECOND CAUSE OF ACTION

Violations of Business & Professions Code § 17200

By Plaintiff and the Class Members Against All Defendants

119. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Complaint as though fully set forth herein.

120. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

121. This cause of action is brought under California Business & Professions Code § 17200 et seq., which prohibits any unlawful, unfair, or fraudulent business act or practice.

122. Defendant has engaged in unlawful business practices by:

(a) Violating California Penal Code §§ 638.50–638.56, including the unauthorized collection of addressing, signaling, and routing information for user identification and tracking; and

(b) Violating California Civil Code § 1798.100, *et seq.*, including collecting, using, and/or selling Plaintiff's and Class Members' personal information and location data to Third Parties without providing sufficient notice. Privacy rights rooted in the CCPA are a protected interest enforceable under Business & Professions Code § 17200. *Briskin v. Shopify, Inc.*, 101 F.4th 706 (9th Cir. 2025) (en banc).

123. Defendant has engaged in unfair business practices by embedding the Trackers into the Website and enabling the real-time capture and transmission of Plaintiff's and Class Members' personal and behavioral information, such as IP address, browser details, visited URLs, referrer paths, timestamps, and interaction events, to the Third Parties.

124. The Defendant's practices are contrary to public policy supporting consumer privacy and data autonomy, and the harm it causes to consumers, including loss of control over personal information and risk of profiling, outweighs any legitimate business justification.

1 125. Defendant has engaged in fraudulent business practices by failing to
2 adequately disclose its data-sharing practices. On information and belief, Defendant
3 omitted material facts from its privacy policy and/or site interface and failed to inform
4 users that their activities would be tracked across the internet and linked to unique
5 identifiers for advertising and profiling purposes. These omissions were likely to
6 deceive a reasonable consumer and were intended to obscure the nature and extent of
7 the surveillance.

8 126. As a direct and proximate result of Defendant's unlawful, unfair, and
9 fraudulent conduct, Plaintiff and the Class Members have suffered injury in fact and
10 loss of money or property, including the unauthorized exfiltration and commodification
11 of valuable personal data. Plaintiff's and Class Members' data—used for targeted
12 advertising, behavioral modeling, and enrichment by third parties—constitutes digital
13 property with measurable economic value.

14 127. Plaintiff on behalf of himself and on behalf of the Class Members seeks
15 injunctive relief to prevent Defendant from continuing its deceptive and unlawful data
16 tracking practices and to require clear and conspicuous notice and opt-in consent for
17 any behavioral tracking involving third-party tools. Plaintiff on behalf of himself and
18 on behalf of the Class Members, also seeks restitution of the value derived from the
19 unauthorized use of their personal information, attorneys' fees where permitted by law,
20 and such other and further relief as the Court may deem just and proper.

21 **IX. PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiff prays for the following:

- 23 1. An order certifying the Class, naming Plaintiff as Class representative,
24 and naming Plaintiff's attorneys as Class counsel;
- 25 2. An order declaring that Defendant's conduct violates CIPA and Business
26 & Professions Code § 17200;
- 27 3. An order of judgment in favor of Plaintiff and the Class against
28 Defendant on the causes of action asserted herein;

4. An order enjoining Defendant's conduct as alleged herein;
5. Statutory damages pursuant to CIPA;
6. Prejudgment interest;
7. Reasonable attorney's fees and costs; and
8. All other relief that would be just and proper as a matter of law or equity.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so permitted.

Dated: July 21, 2025

NATHAN & ASSOCIATES, APC

By: /s/ Reuben D. Nathan

Reuben D. Nathan, Esq.
Attorneys for Plaintiff