Reuben D. Nathan, Esq. (SBN 208436)
NATHAN & ASSOCIATES, APC
2901 W. Coast Hwy., Suite 200
Newport Beach, CA 92663
Office: (949) 270-2798
Email: rnathan@nathanlawpractice.com

Ross Cornell, Esq. (SBN 210413)
LAW OFFICES OF ROSS CORNELL, APC
40729 Village Dr., Suite 8 - 1989
Big Bear Lake, CA 92315
Office: (562) 612-1708
Email: rc@rosscornelllaw.com

Attorneys for Plaintiff: AUSTIN WHITE

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AUSTIN WHITE, on behalf of himself and all similarly situated persons, Plaintiff, v. ETSY, INC., Defendants.	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. Defendant ETSY, INC. (collectively referred to herein as "Defendant" or "ETSY") own and operate a website, www.etsy.com (the "Website").

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

3. Plaintiff AUSTIN WHITE files this class action complaint on behalf of himself and all others similarly situated (the "Class Members") against Defendant. Plaintiff brings this action based upon personal knowledge of the facts pertaining to him, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

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

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

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

- Google Ads/DoubleClick Tracker
- Facebook PixelTracker
- TikTok Tracker
- Bing/Microsoft Ads Tracker
- The Trade Desk Tracker
- Qualtrics Tracker
- Podscribe Tracker

/ /

7. The third parties who operate the above-listed trackers use pieces of User Information (defined below) collected via the Website as described herein for their own independent purposes tied to broader advertising ecosystems, profiling, and data monetization strategies that go beyond Defendant's direct needs for their own financial gain. The above-listed trackers are referred to herein collectively as the "Trackers."

- The Trackers are operated by distinct third parties: Google LLC (Google Ads / DoubleClick Tracker); Meta Platforms, Inc. (Facebook Pixel Tracker); TikTok Inc. (TikTok Tracker); Microsoft Corporation (Bing / Microsoft Ads Tracker); The Trade Desk, Inc. (The Trade Desk Tracker); Qualtrics, LLC (Qualtrics Tracker); and Podscribe, Inc. (Podscribe Tracker). Defendant enables these trackers, which transmit user data to third-party servers to identify users and support advertising, profiling, and data monetization activities.

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

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

10. Plaintiff and the Class Members did not consent to the installation, execution, embedding, or injection of the Trackers on their devices and did not expect their behavioral data to be disclosed or monetized in this way. By installing and using

the Trackers without prior consent and without a court order, Defendant violated CIPA section 638.51.

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

12. Defendant provides a privacy policy referred to as "House Rules" on the Website (the "Privacy Policy") but does not conform to the Privacy Policy:

a. Defendant represents that it engages third-party companies and individuals to help operate, provide, and advertise its services and that such third parties have limited access to personal information and are only permitted to use personal information to perform the identified tasks on Defendant's behalf and are prohibited from disclosing or using personal information for other purposes. Defendant claims limited, purpose-bound sharing, which is inconsistent with the broad dissemination of tracking data to third-party adtech ecosystems with no indication of real-time constraint enforcement.

b. Defendant does not clearly disclose that real-time behavioral data is transmitted to third parties immediately upon site arrival;

c. Defendant represents that the Website uses data analytics software to improve its services and that Defendant relies on consumer consent to personalize advertisements on third-party platforms. In reality, the Website provides no initial consent mechanism

d. Tracking and third-party sharing occurs prior to presenting users with a valid choice to opt-out or manage consent;

/ /

/ /

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

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

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

II. PARTIES

15. Plaintiff AUSTIN WHITE ("Plaintiff") is a California citizen residing in Alameda 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 October 20, 2024, and during which time Plaintiff submitted private information on the Website in order to complete a purchase from ETSY with a credit card. The allegations set forth herein are based on the Website as configured when Plaintiff visited it.

16. Defendant ETSY, INC. is a Delaware corporation that owns, operates and/or controls the Website which is an online platform that offers goods and services to consumers.

17. ETSY is a leading global e-commerce marketplace focused on handmade goods, vintage items, and craft supplies. The company maintains a dominant online presence in the United States and operates its primary consumer platform at www.etsy.com. Headquartered at 117 Adams Street, Brooklyn, New York, ETSY enables users to browse and purchase millions of unique products from independent sellers around the world.

18. ETSY functions as the flagship consumer-facing brand of Etsy, Inc.'s broader commercial ecosystem. While the company supports a variety of seller tools and services, the ETSY platform is directly responsible for facilitating marketplace transactions, processing customer payments, and managing communications between

buyers and sellers. In the course of operating its online marketplace, ETSY collects and processes significant volumes of user data for purposes that include transaction fulfillment, behavioral profiling, and digital advertising, all of which give rise to obligations under California and federal privacy law.

19. The Website serves as ETSY's primary digital storefront. It allows users to explore product listings, save favorites, manage accounts, and complete purchases. In addition to these retail functions, the Website also operates as a behavioral tracking and advertising platform. Through the deployment of third-party tracking technologies including advertising pixels, event tracking scripts, behavioral monitoring tools, and data brokering integrations ETSY collects granular data about user interactions with the site. These data practices form a core component of ETSY's performance marketing, ad-targeting, and audience monetization strategy, and raise serious legal concerns under the California Invasion of Privacy Act (CIPA) and other consumer privacy statutes.

III. <u>JURISDICTION AND VENUE</u>

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

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

22. Venue is proper in the Northern District of California pursuant to 28 U.S.C. § 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. <u>GENERAL ALLEGATIONS</u>

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

23. 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).

24. 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)).

25. 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)).

26. 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)).

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

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

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

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

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

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

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

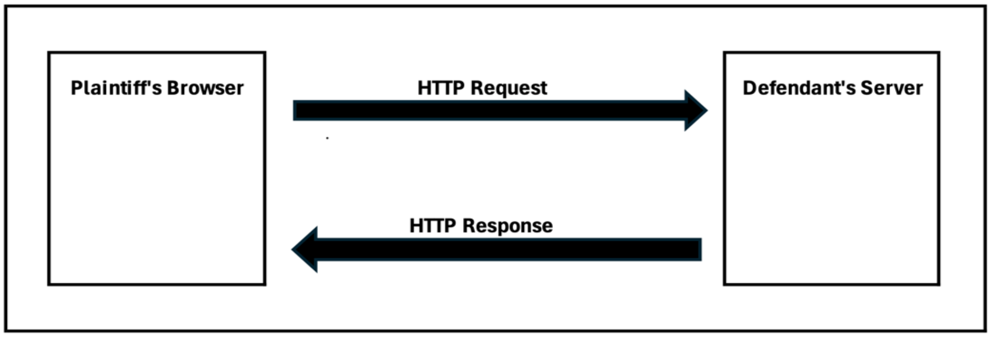
34. Individuals may pursue legal action against violators of any CIPA provision, including Section 638.51, and are entitled to seek $5,000 in statutory penalties per violation (Cal. Penal Code § 637.2(a)(1)).

/ /

2. *The Trackers Are "Pen Registers" and/or "Trap and Trace Devices"*

35. 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



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

37. The Trackers operate by initiating HTTP or HTTPS requests—using either the GET or POST method from the user's browser to external servers controlled

by the Third Parties. These requests are triggered automatically during the page load and by user interactions with the Website. They are used to transmit behavioral data and device metadata, including information such as page views, click events, session duration, and identifying browser characteristics.

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

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

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

41. Public IP addresses play a significant role in digital marketing by enabling geographic targeting based on a user's approximate location. Through IP geolocation services, advertisers can often determine a user's country, region, city, and in some cases, ZIP code or service area. In contexts where a static IP address is associated with a fixed residence or business, this data can contribute to household-level or business-level targeting, particularly when combined with other tracking identifiers and third-party enrichment.

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

43. As "routing, addressing, or signaling information," a public IP address is indispensable for maintaining seamless and efficient communication over the Internet. It ensures that data packets are sent from the user's router to the intended destination, such as a website or email server.

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

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

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

46. This process, known as digital fingerprinting, involves compiling various data points such as browser version, screen resolution, installed fonts, device type, and language settings to generate a unique identifier for each user. Fingerprinting can be used to recognize repeat visits and correlate activity across different sessions or sites. When combined with form inputs, login activity, or third-party enrichment,

fingerprinting can contribute to broader profiling of a user's interests, affiliations, or behaviors.

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

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

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

50. The Trackers provide analytics and marketing services to Defendant using the data collected from visitors to the Website. These services also leverage user data collected from other websites that include the same pen register and trap and trace devices operated by the Third Parties.

/ /

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

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

52. Given the number of Internet users, the "world's most valuable resource is no longer oil, but data."[1]

53. Consumers' web browsing histories have an economic value more than $52 per year, while their contact information is worth at least $4.20 per year, and their demographic information is worth at least $3.00 per year.[2]

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

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

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

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

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

businesses that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

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

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

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

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

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

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

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

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

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

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

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

62. 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).

63. 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*

64. When a user visits the Website, a suite of background tracking technologies is activated immediately upon page load. These include client-side scripts deployed by third-party Trackers, which begin collecting various categories of User Information without any visible indication to the user. Together, these technologies function as a coordinated data collection infrastructure that allows Defendant to analyze user behavior at a highly granular level and to leverage that insight in real time for marketing optimization, user targeting, and business intelligence.

65. On information and belief, the Trackers operate as part of a vast and interconnected digital advertising ecosystem, and these entities leverage shared

identifiers, cookie syncing, and cross-device tracking techniques to follow users across websites, platforms, and environments, with tools specifically engineered to build persistent consumer profiles, enabling real-time behavioral targeting and identity resolution at scale.

66. On the Website, a coordinated network of third-party trackers is deployed to facilitate identity resolution, targeted advertising, and data monetization. This infrastructure includes both trackers embedded directly in the page's HTML and others deployed through JavaScript-based execution during runtime. Google Ads / DoubleClick, the Facebook Pixel Tracker, TikTok Tracker, and Bing / Microsoft Ads Tracker are embedded in the initial page source and activate immediately upon page load. Additional trackers including The Trade Desk Tracker and Qualtrics Tracker, are dynamically injected using JavaScript functions that execute during or shortly after the initial page load process. These technologies operate in tandem to collect and transmit user interaction data in real time, supporting downstream advertising, profiling, and data-sharing operations.

67. Identity resolution on the Website is primarily facilitated through the interplay of the Facebook Pixel Tracker, TikTok Tracker, and Qualtrics Tracker. The Facebook Pixel Tracker identifies users by linking on-site behavior to existing Facebook cookies and logged-in sessions, enabling the correlation of browsing activity with social media identities. The TikTok Tracker collects device-level information and leverages both browser fingerprinting and cookie-based identifiers to associate user activity with persistent profiles on the TikTok platform. The Qualtrics Tracker contributes to identity resolution through behavioral segmentation and targeting logic designed to match users with audience categories in real time. These combined technologies enable ETSY to de-anonymize users over time, correlate behaviors with known identities, and build detailed demographic and behavioral profiles.

68. Once identity signals are gathered, targeted advertising and data monetization are executed through platforms such as Google Ads / DoubleClick, The

Trade Desk, and Bing / Microsoft Ads. These entities participate in real-time bidding (RTB) and programmatic advertising markets, enabling ETSY to auction access to users based on behavioral and identity-linked data. Google Ads / DoubleClick delivers performance-based advertising by leveraging browsing behavior, conversion history, and demographic profiles to serve targeted creatives. The Trade Desk acts as a demand-side platform (DSP), facilitating cross-channel ad buying and real-time audience targeting. Bing / Microsoft Ads uses conversion tracking and event-level data to enable remarketing and audience segmentation across Microsoft's advertising ecosystem. Together, these trackers convert user interactions into marketable audience segments, driving measurable advertising outcomes and monetization for ETSY.

69. Defendant shares User Information with third-party advertising platforms, including DoubleClick. These platforms operate real-time bidding systems that auction ad space to the highest bidder using behavioral data collected from users during their visit to the Website. When a user loads the Website, data is immediately transmitted to DoubleClick and related ad services without any action or consent from the user. This includes the user's internet protocol address, browser type, device information, and the URL of the page visited. These identifiers enable advertisers to track users across websites, build behavioral profiles, and deliver personalized advertising in real time.

70. Network requests to DoubleClick's activity and view through conversion endpoints demonstrate Defendant's participation in an integrated advertising architecture that supports real-time ad placement. This system enables advertisers to bid for ad impressions based on user characteristics, allowing Defendant to increase ad revenue by monetizing user attention. These exchanges serve no functional purpose for the user; their sole role is to maximize Defendant's advertising returns. By embedding tracking requests that operate silently and immediately on page load, Defendant treats personal data as a commodity for its own profit.

/ /

V. SPECIFIC ALLEGATIONS

1. Google Ads / DoubleClick Tracker

71. 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.

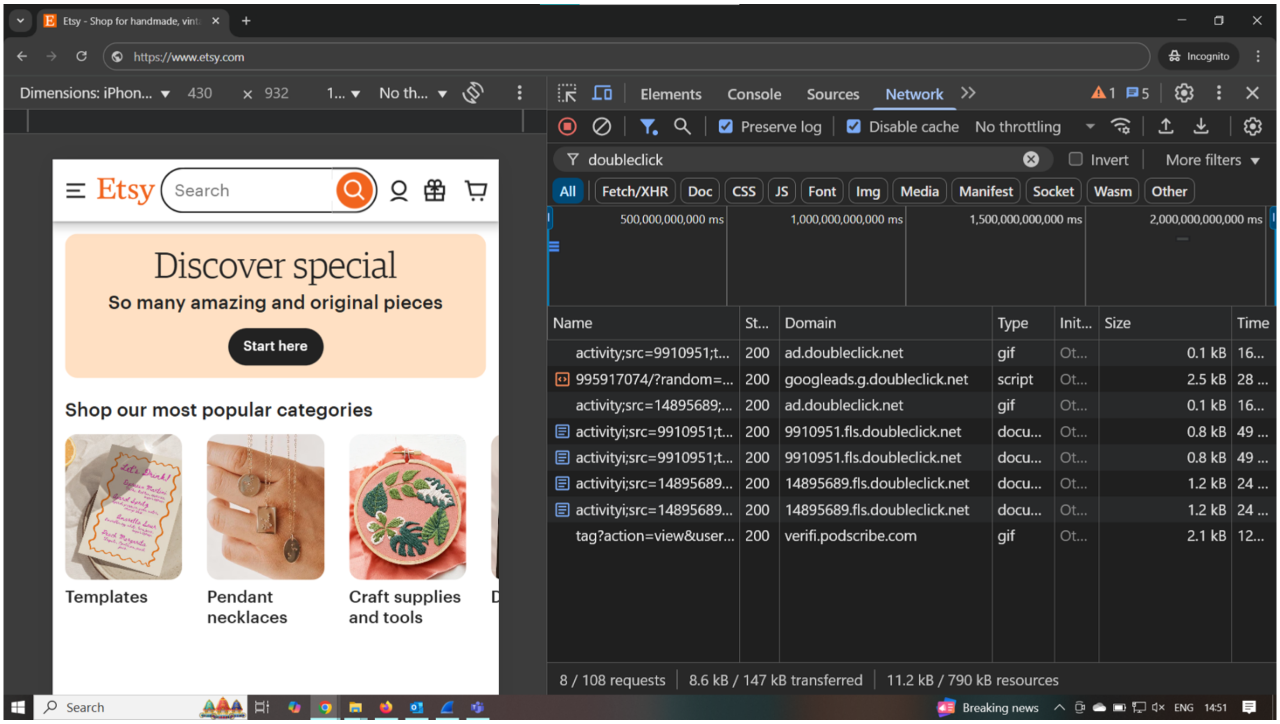
72. When implemented on the Website, the Google Ads / DoubleClick Tracker collects a broad set of user metadata, including visited URLs, session timestamps, referrer headers, and in-page activity data such as page views and navigation events. It also captures technical device attributes such as IP address, 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 / DoubleClick 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.

73. The Google Ads / DoubleClick 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 / DoubleClick 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.

/ /

74. ***Figure 2*** below is a screenshot from the Website, confirming that the Google Ads / DoubleClick Tracker was triggered automatically upon visiting the homepage. Multiple GET and document requests to domains including ad.doubleclick.net and fls.doubleclick.net were initiated during the initial session and returned 200 OK status codes. These requests reflect tracking endpoints used by Google's advertising infrastructure to deliver behavioral tracking scripts and log session-level activity. This network activity occurred prior to any user interaction, confirming that the Google Ads / DoubleClick Tracker was active upon page load.

Figure 2



☑ Preserve log ☑ Disable cache No throttling

doubleclick

□ Invert More filters

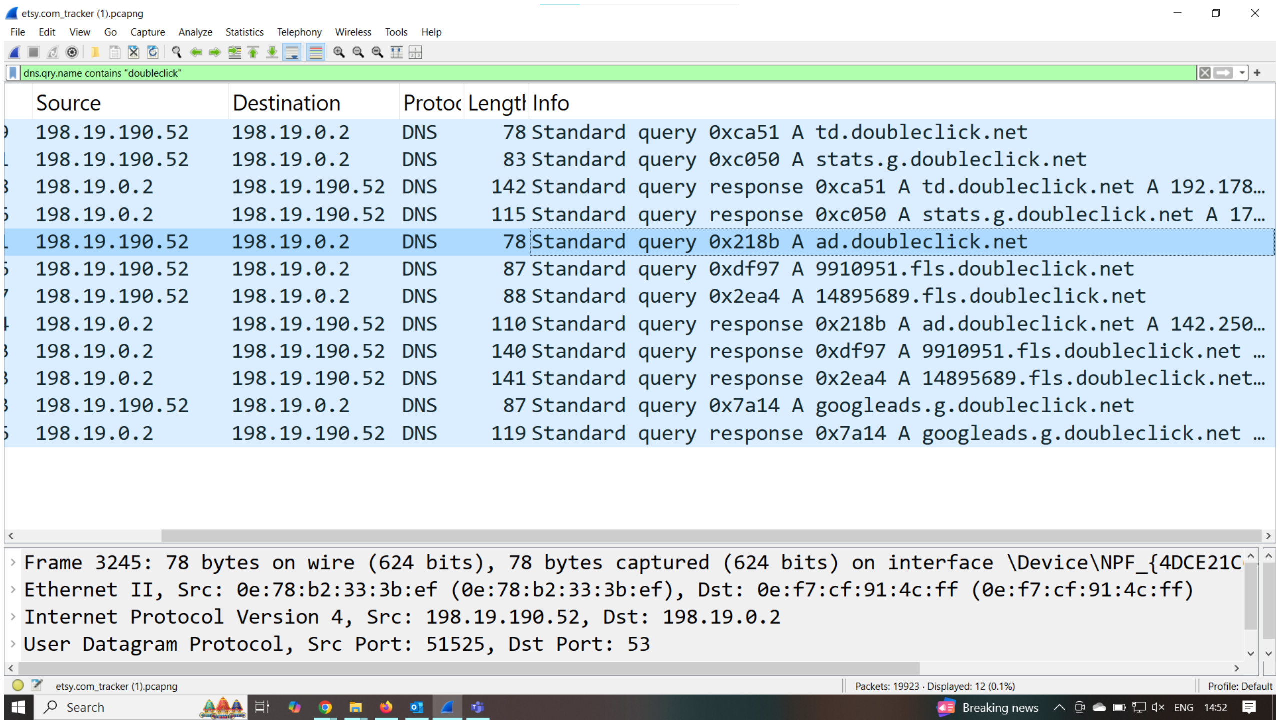
Name	St...	Domain	Type	Init...	Size	Time
activity;src=9910951;t...	200	ad.doubleclick.net	gif	Ot...	0.1 kB	16...
995917074/?random=...	200	googleads.g.doubleclick.net	script	Ot...	2.5 kB	28 ...
activity;src=14895689;...	200	ad.doubleclick.net	gif	Ot...	0.1 kB	16...
activityi;src=9910951;t...	200	9910951.fls.doubleclick.net	docu...	Ot...	0.8 kB	49 ...
activityi;src=9910951;t...	200	9910951.fls.doubleclick.net	docu...	Ot...	0.8 kB	49 ...
activityi;src=14895689...	200	14895689.fls.doubleclick.net	docu...	Ot...	1.2 kB	24 ...
activityi;src=14895689...	200	14895689.fls.doubleclick.net	docu...	Ot...	1.2 kB	24 ...
tag?action=view&user...	200	verifi.podscribe.com	gif	Ot...	2.1 kB	12...

8 / 108 requests | 8.6 kB / 147 kB transferred | 11.2 kB / 790 kB resources

75. ***Figure 3*** below is a screenshot of network activity on the Website, capturing DNS queries and corresponding responses for multiple subdomains of doubleclick.net, including td.doubleclick.net, stats.g.doubleclick.net, ad.doubleclick.net, fls.doubleclick.net, and googleads.g.doubleclick.net. These DNS transactions confirm that the Website initiated background DNS resolution of Google's advertising infrastructure during the user's initial session. The DNS activity occurred

prior to any user interaction, confirming that the Google Ads / DoubleClick Tracker was silently activated upon page load.

Figure 3



etsy.com_tracker (1).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns.qry.name contains "doubleclick"
```

```
Source          Destination     Protoc Lengtl Info
198.19.190.52   198.19.0.2      DNS      78 Standard query 0xca51 A td.doubleclick.net
198.19.190.52   198.19.0.2      DNS      83 Standard query 0xc050 A stats.g.doubleclick.net
198.19.0.2      198.19.190.52   DNS     142 Standard query response 0xca51 A td.doubleclick.net A 192.178…
198.19.0.2      198.19.190.52   DNS     115 Standard query response 0xc050 A stats.g.doubleclick.net A 17…
198.19.190.52   198.19.0.2      DNS      78 Standard query 0x218b A ad.doubleclick.net
198.19.190.52   198.19.0.2      DNS      87 Standard query 0xdf97 A 9910951.fls.doubleclick.net
198.19.190.52   198.19.0.2      DNS      88 Standard query 0x2ea4 A 14895689.fls.doubleclick.net
198.19.0.2      198.19.190.52   DNS     110 Standard query response 0x218b A ad.doubleclick.net A 142.250…
198.19.0.2      198.19.190.52   DNS     140 Standard query response 0xdf97 A 9910951.fls.doubleclick.net …
198.19.0.2      198.19.190.52   DNS     141 Standard query response 0x2ea4 A 14895689.fls.doubleclick.net…
198.19.190.52   198.19.0.2      DNS      87 Standard query 0x7a14 A googleads.g.doubleclick.net
198.19.0.2      198.19.190.52   DNS     119 Standard query response 0x7a14 A googleads.g.doubleclick.net …
```

```
> Frame 3245: 78 bytes on wire (624 bits), 78 bytes captured (624 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)
> Internet Protocol Version 4, Src: 198.19.190.52, Dst: 198.19.0.2
> User Datagram Protocol, Src Port: 51525, Dst Port: 53
```

etsy.com_tracker (1).pcapng
Packets: 19923 · Displayed: 12 (0.1%)
Profile: Default
Search
Breaking news
ENG
14:52

76. 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.

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

78. 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).

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

80. 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 Google Ads / DoubleClick Tracker on Plaintiff's and Class Members' browser or to collect or share data with Google.

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

2. The Facebook Pixel Tracker

82. The Facebook Pixel Tracker is a behavioral tracking script implemented through Meta's Pixel technology, typically delivered via domains such as connect.facebook.net and facebook.com/tr/. On the Website, the Facebook Pixel Tracker is injected through tag management infrastructure. Once loaded, it initiates background communication with Meta's servers and enables real-time tracking of user activity.

83. On the Website's homepage, the Facebook Pixel Tracker activates automatically upon page load and begins capturing behavioral data in real time. It records interaction signals such as page views and other engagement events without requiring any user action. The Facebook Pixel Tracker actively detects and collects additional user interaction, including click-based events and scrolling behavior. These signals are transmitted to Meta's servers and associated with the user's Facebook or

Instagram profile, even if the user never directly interacts with any Meta service while on the Website.

84. The data collected by the Facebook Pixel Tracker supports identity resolution by linking behavioral data from the Website with individual user profiles across Meta's platforms. If the user is logged into Facebook, Instagram, or Messenger on the same device or browser, the Facebook Pixel Tracker can tie Website behavior to the user's unique Meta ID. Even if not logged in, Meta can assign a persistent identifier using cookies, browser fingerprinting, or pixel fire data. This enables the creation of robust cross-site behavioral profiles based on a user's activity on ETSY's website.

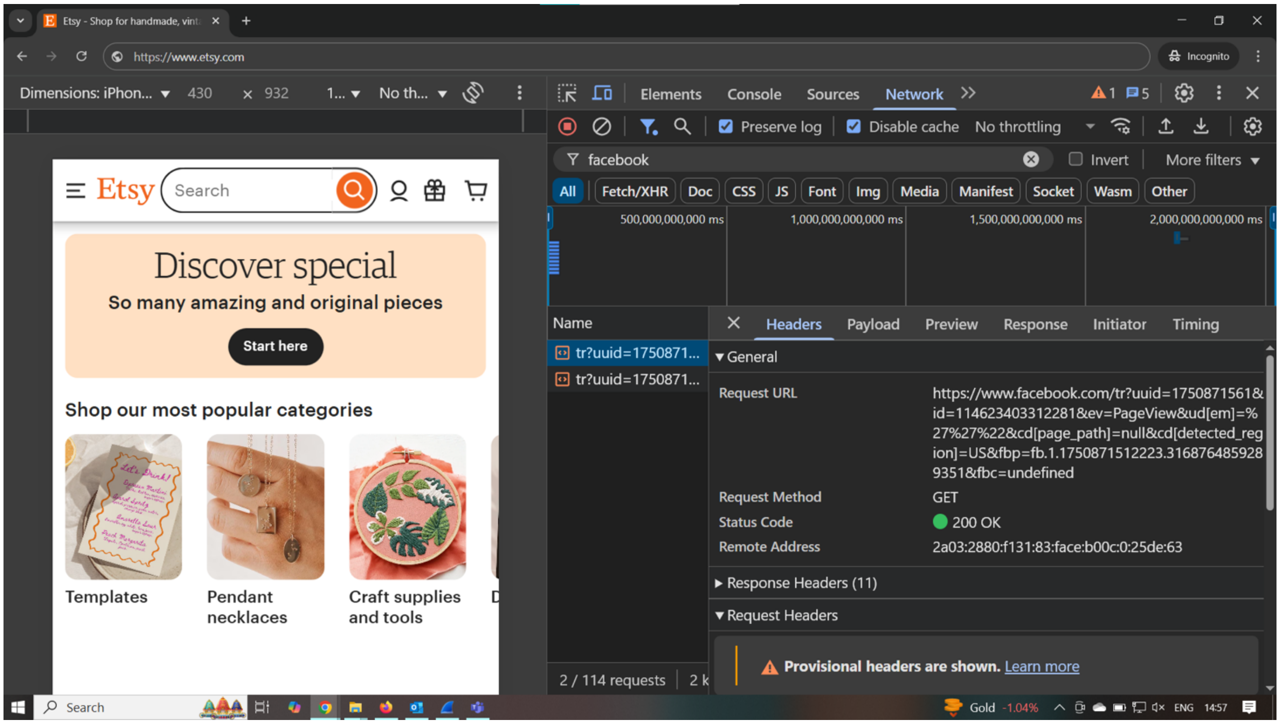
85. The Facebook Pixel Tracker also serves ETSY's goal of targeted advertising by enabling the creation of "Custom Audiences,"groups of users who have taken specific actions on the Website, such as browsing listings, viewing product pages, or beginning a checkout process. ETSY can then use Meta's Ads Manager to re-target those users across Facebook and Instagram, or to generate "Lookalike Audiences" that mirror the behavioral patterns of existing visitors. These mechanisms allow ETSY to efficiently deliver marketing content to users most likely to engage or convert.

86. The Facebook Pixel Tracker contributes to ETSY's data monetization strategy by turning behavioral insights into measurable advertising ROI. The Facebook Pixel Tracker generates real-time analytics regarding user behavior, campaign performance, and conversion attribution, which Meta then delivers to ETSY through its Ads infrastructure. This closed-loop feedback system connects on-site engagement with off-site ad delivery, allowing ETSY to refine ad spend, personalize messaging, and increase the value of each user interaction. In this way, the Facebook Pixel Tracker functions as a core part of ETSY's commercial surveillance infrastructure.

87. ***Figure 4*** below is a screenshot from the Website, confirming that the Facebook Pixel Tracker was triggered during the user's session on the homepage. A request to www.facebook.com was initiated by JavaScript code delivered through Google Tag Manager (gtm.js), and the request returned a 200 status. This

communication with Meta's tracking infrastructure occurred automatically and before any user interaction, verifying that the Facebook Pixel Tracker was active and collecting behavioral data in the background.

Figure 4



▾ General

Request URL: https://www.facebook.com/tr?uuid=1750871561&id=1146234033122818&ev=PageView&ud[em]=%27%27%22&cd[page_path]=null&cd[detected_region]=US&fbp=fb.1.1750871512223.3168764859289351&fbc=undefined

Request Method: GET

Status Code: ● 200 OK

Remote Address: 2a03:2880:f131:83:face:b00c:0:25de:63

▸ Response Headers (11)

▾ Request Headers

⚠ Provisional headers are shown. Learn more

88. ***Figure 5*** below is a screenshot of network activity on the Website, capturing a DNS query and corresponding response for www.facebook.com. This confirms that the Website initiated background DNS resolution of Meta's tracking infrastructure during the user's session on the homepage. The DNS activity was automatically generated and occurred without any user interaction, further demonstrating that the Facebook Pixel Tracker was operating silently in the background.

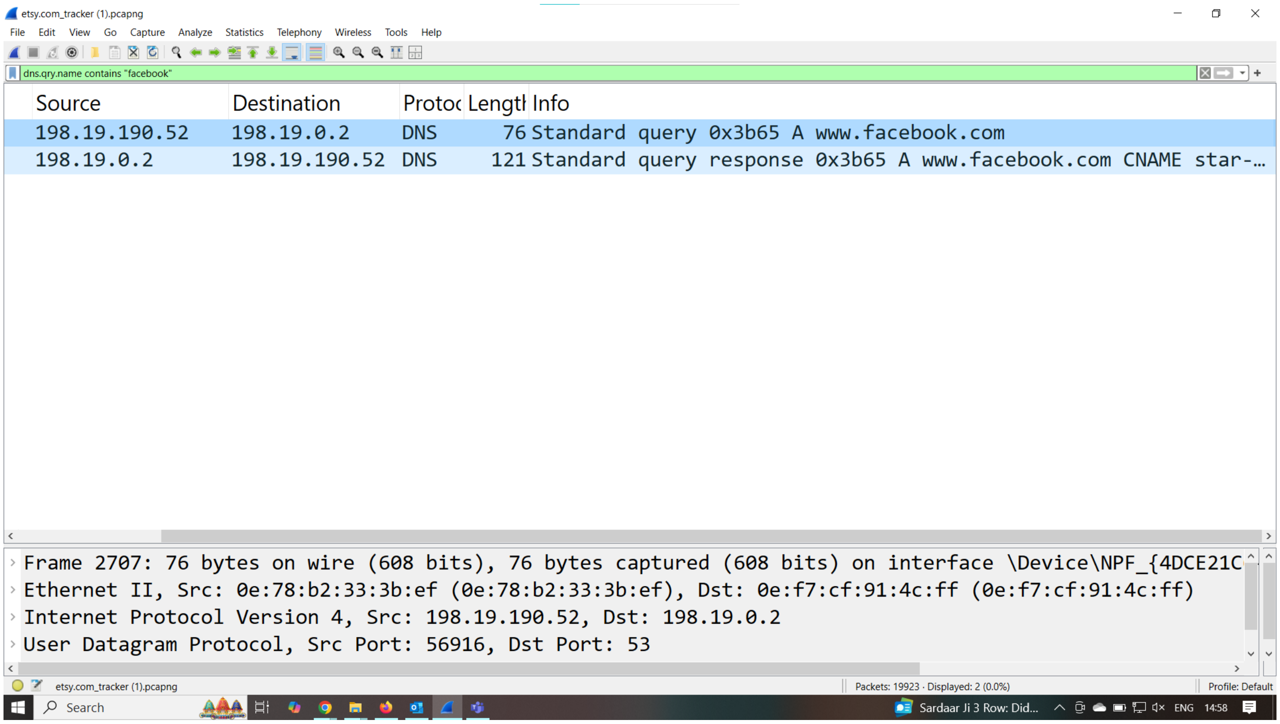
/ /

/ /

/ /

/ /

Figure 5


etsy.com_tracker (1).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Search
Sardaar Ji 3 Row: Did...
ENG
14:58

dns.qry.name contains "facebook"

```
Source          Destination     Protoc Lengtl Info
198.19.190.52   198.19.0.2      DNS       76 Standard query 0x3b65 A www.facebook.com
198.19.0.2      198.19.190.52   DNS      121 Standard query response 0x3b65 A www.facebook.com CNAME star-…
```

```
› Frame 2707: 76 bytes on wire (608 bits), 76 bytes captured (608 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)
› Internet Protocol Version 4, Src: 198.19.190.52, Dst: 198.19.0.2
› User Datagram Protocol, Src Port: 56916, Dst Port: 53
```

etsy.com_tracker (1).pcapng | Packets: 19923 · Displayed: 2 (0.0%) | Profile: Default

89. 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.

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

91. The Facebook Pixel 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).

92. The Facebook Pixel Tracker captures and transmits routing, addressing, and signaling information such as the user's page URL, referrer, and browser metadata

to Meta's servers as soon as the page loads, without the user's knowledge or consent. This type of metadata reveals the origin and destination of the user's electronic communications. The connection is not initiated by the user, but rather by code embedded in the Website, allowing Meta to intercept and associate those signals with a known or inferred identity. The transmission occurs while the user's communication is still in transit and is diverted to Meta without authorization.

93. 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 Facebook Pixel Tracker on Plaintiff's and Class Members' browser or to collect or share data with Facebook.

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

3. The TikTok Tracker

95. The TikTok Tracker is a piece of software code that Defendant placed on the Website to share user interaction data and other Website events with TikTok. The TikTok Tracker enables the transmission of behavioral signals and technical metadata to TikTok's tracking infrastructure, allowing TikTok to monitor activity on the Website in real time.

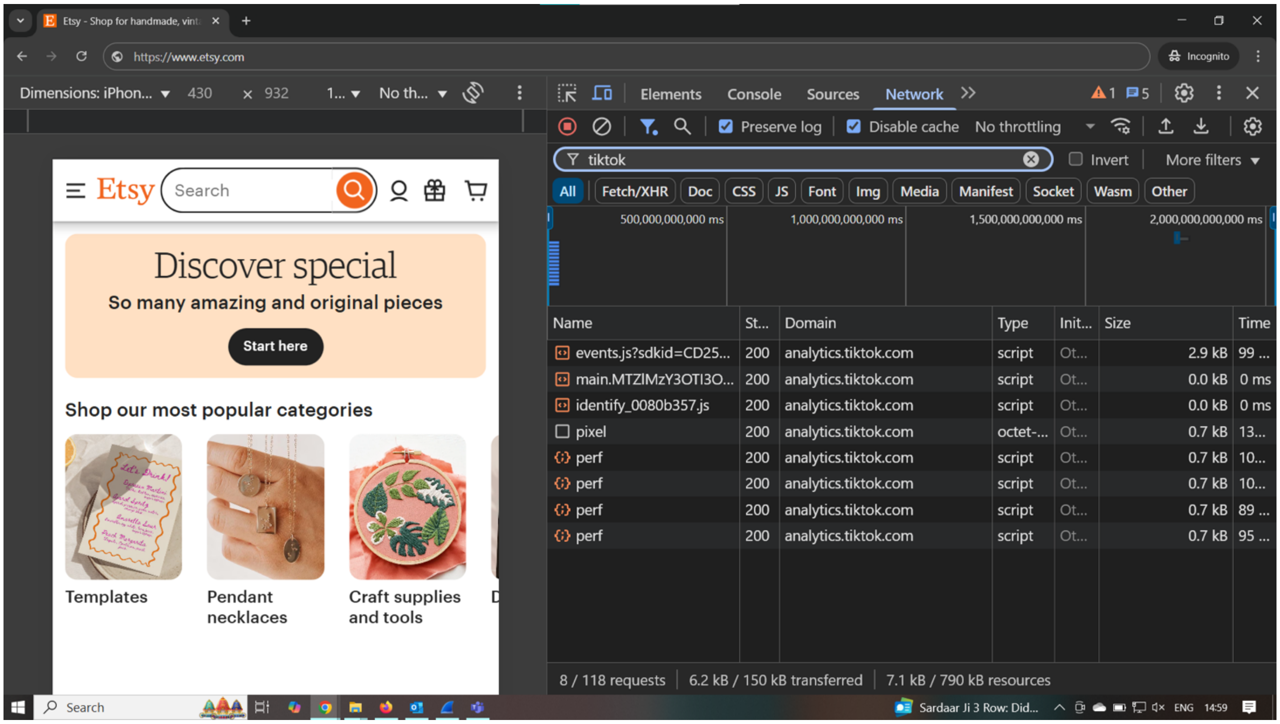
96. The TikTok Tracker uses pixel-based surveillance mechanisms to collect and process user data in real time. It monitors interactions on the Website, including page views and actions taken on specific listings or interface elements. This data is used to analyze advertising performance, conduct behavioral targeting, and drive revenue through the covert capture and transmission of user information including that of Plaintiffs and Class Members to TikTok's tracking infrastructure.

97. The TikTok Tracker begins collecting information immediately upon the user's arrival on the Website. It gathers device and browser attributes, IP-based geolocation data, HTTP referrer headers, and the URL of the page visited. This

information is transmitted to TikTok in real time using JavaScript-based tracking scripts. TikTok acknowledges that the TikTok tracker automatically collects Plaintiff and Class Members' IP address and sends that information to TikTok.[7]

98. ***Figure 6*** below is a screenshot from the Website, confirming that the TikTok Tracker was triggered automatically upon visiting the homepage. Multiple script and ping requests to analytics.tiktok.com were initiated by JavaScript code running on the site, including to endpoints such as /i18n/pixel/events.js, /pixel, and /identify. These requests were executed without any user interaction, returned HTTP 200 status codes, and demonstrate that the TikTok Tracker was actively communicating with TikTok's infrastructure during the initial homepage session.

Figure 6



Name	St...	Domain	Type	Init...	Size	Time
events.js?sdkid=CD25...	200	analytics.tiktok.com	script	Ot...	2.9 kB	99 ...
main.MTZlMzY3OTI3O...	200	analytics.tiktok.com	script	Ot...	0.0 kB	0 ms
identify_0080b357.js	200	analytics.tiktok.com	script	Ot...	0.0 kB	0 ms
pixel	200	analytics.tiktok.com	octet-...	Ot...	0.7 kB	13...
perf	200	analytics.tiktok.com	script	Ot...	0.7 kB	10...
perf	200	analytics.tiktok.com	script	Ot...	0.7 kB	10...
perf	200	analytics.tiktok.com	script	Ot...	0.7 kB	89 ...
perf	200	analytics.tiktok.com	script	Ot...	0.7 kB	95 ...

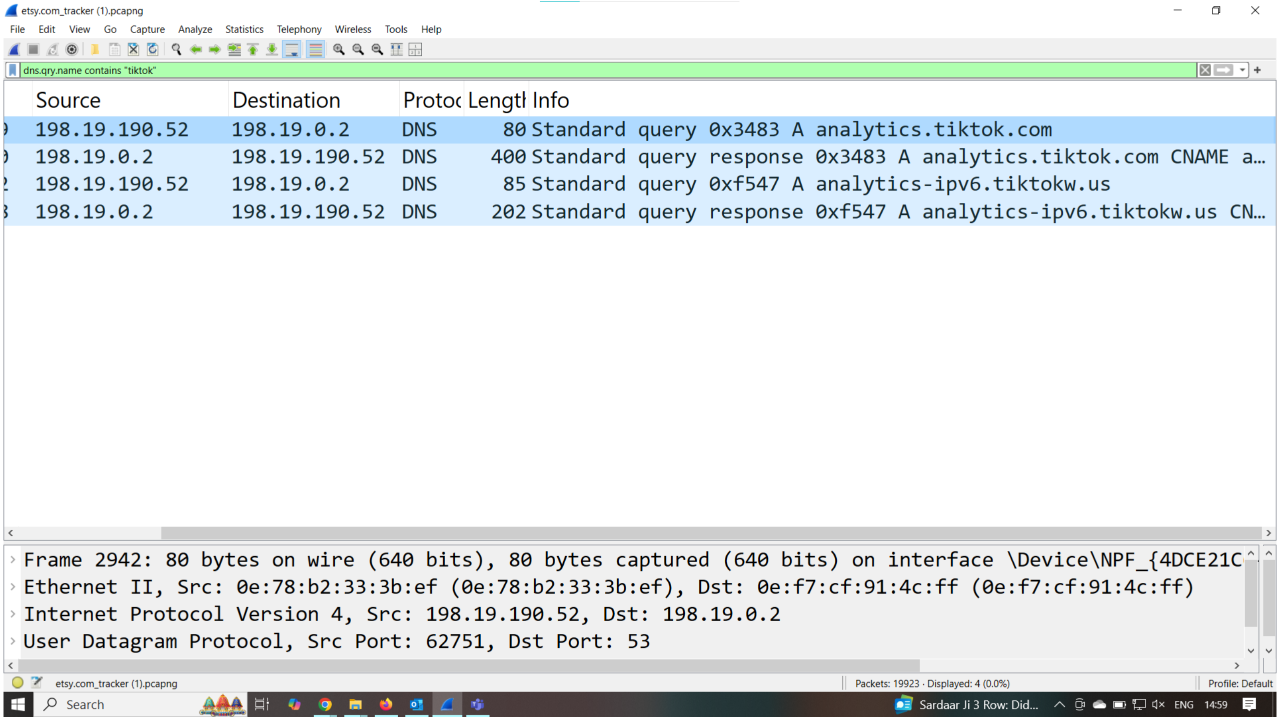
8 / 118 requests | 6.2 kB / 150 kB transferred | 7.1 kB / 790 kB resources

99. ***Figure 7*** below is a screenshot of network activity on the Website, capturing a DNS query and corresponding response for analytics.tiktok.com. This confirms that the Website resolved TikTok's tracking domains: analytics.tiktok.com,

[7] https://ads.tiktok.com/help/article/tiktok-pixel?q=tiktok%20pixel&redirected=1

analytics.tiktok.com CNAME, analytics.ipv6.tiktok.com, and analytics.ipv6.tiktok.us during the user's homepage session. The DNS request was automatically triggered without any user interaction, further demonstrating that the TikTok Tracker was operating silently in the background.

Figure 7


etsy.com_tracker (1).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains "tiktok"

```
  Source          Destination     Protoc Lengtl Info
) 198.19.190.52   198.19.0.2      DNS        80 Standard query 0x3483 A analytics.tiktok.com
) 198.19.0.2      198.19.190.52   DNS       400 Standard query response 0x3483 A analytics.tiktok.com CNAME a…
2 198.19.190.52   198.19.0.2      DNS        85 Standard query 0xf547 A analytics-ipv6.tiktokw.us
3 198.19.0.2      198.19.190.52   DNS       202 Standard query response 0xf547 A analytics-ipv6.tiktokw.us CN…
```

```
> Frame 2942: 80 bytes on wire (640 bits), 80 bytes captured (640 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)
> Internet Protocol Version 4, Src: 198.19.190.52, Dst: 198.19.0.2
> User Datagram Protocol, Src Port: 62751, Dst Port: 53
```

etsy.com_tracker (1).pcapng | Packets: 19923 · Displayed: 4 (0.0%) | Profile: Default

100. The collection of Plaintiff's and Class Members' personally identifying and non-anonymized information through Defendant's installation and use of the TikTok Tracker constitutes an invasion of privacy and violates CIPA. Cal. Penal Code § 638.51(a).

101. According to a leading data security firm, the TikTok tracker secretly installed on the Website is particularly invasive. The Tik Tok tracker "immediately links to data harvesting platforms that pick off usernames and passwords, credit card and banking information and details about users' personal health." The pixel also collects "names, passwords and authentication codes" and "transfer the data to locations around the globe, including China and Russia", and does so "before users have a chance

to accept cookies or otherwise grant consent."[8]

102. The TikTok tracker runs on virtually every page of Defendant's Website, sending to TikTok information regarding the Website user's interest in Defendant's products and/or services.

103. The Website transmits tracking signals to TikTok immediately upon page load and continues to initiate communications with TikTok's servers when a user navigates between pages. These transmissions allow TikTok to persistently track user activity across multiple areas of the Website during a single session.

104. The TikTok Tracker facilitates identity resolution by collecting browser metadata, device identifiers, and behavioral signals from users' sessions on the Website. These data points including IP addresses, user-agent strings, session timing, and specific pageview events are transmitted to TikTok's servers immediately upon page load. TikTok uses this information to associate user activity with persistent identifiers across sessions and devices. Even when users are not logged into a TikTok account, the Tracker enables the construction of behavioral profiles and the inference of user identity through fingerprinting techniques and unique tracking parameters.

105. By sharing Plaintiff's and Class Members' personal and de-anonymized data with TikTok, Defendant effectively "doxed" them to America's most formidable geopolitical adversary without informing them that the Website is collaborating with the Chinese government to obtain their identifying information. By sharing Plaintiff's and Class Members' personal and de-anonymized data with TikTok, Defendant effectively "doxed" them to America's most formidable geopolitical adversary. There is evidence that sharing data with TikTok, whose parent company ByteDance, has drawn national security scrutiny. Former employees have testified that data stored on TikTok systems was accessible by ByteDance staff in China.

[8] Aaron Katersky, TikTok Has Your Data Even If You've Never Used The App: Report, ABC News (last accessed October 2024), https://abcnews.go.com/Business/tiktok-data-app-report/story?id=97913249

106. Defendant surreptitiously installed, executed, embedded, or injected the TikTok Tracker by deploying TikTok's JavaScript tracking code through dynamic injection on the Website. When a user visits the Website, their browser executes the script, which transmits data about the user's interactions including the user's IP address, page URL, and other metadata to TikTok's servers. This communication occurs silently and automatically, without any user action or awareness.

107. The TikTok Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

108. The TikTok 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).

109. The TikTok tracker functions as a pen register or trap and trace device because it is designed to capture and transmit addressing, signaling, and routing information associated with a user's interactions on a website, including such information as page URLs, video identifiers, device and browser metadata, IP address, click paths, scroll depth, and session timestamps. This data reveals the origin and destination of electronic communications, closely analogous to how a traditional pen register captures dialed numbers and a trap and trace device records incoming call data. By systematically logging which content the user accessed (i.e., the "addressed" destination), the technical attributes of the user's system (i.e., the "signaling"), and the communication route (i.e., IP routing and timestamps), the TikTok tracker enables TikTok to identify patterns of communication behavior, monitor content consumption in real time, and attribute it to specific individuals or devices.

110. 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 TikTok Tracker on Plaintiff's and Class Members' browser or to collect or share data with TikTok.

/ /

111. Consequently, the Defendant's secret installation of the TikTok tracker violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

4. The Bing / Microsoft Ads Tracker

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

113. The Bing / Microsoft Ads Tracker is designed to silently collect a range of user data when a visitor lands on the Website. It gathers device and browser metadata, IP address, estimated geolocation, referrer URLs, and viewed pages. It is also designed 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.

114. ***Figure 8*** below is a screenshot from the Website, confirming that the Bing / Microsoft Ads Tracker was triggered during the user's session on the homepage. Multiple script requests to bat.bing.com were initiated during the initial session and returned 200 status codes. These requests, which included files such as bat.js and related script variants, were executed without any user interaction. This confirms that Microsoft's tracking infrastructure was activated automatically upon page load and was collecting session data in the background.

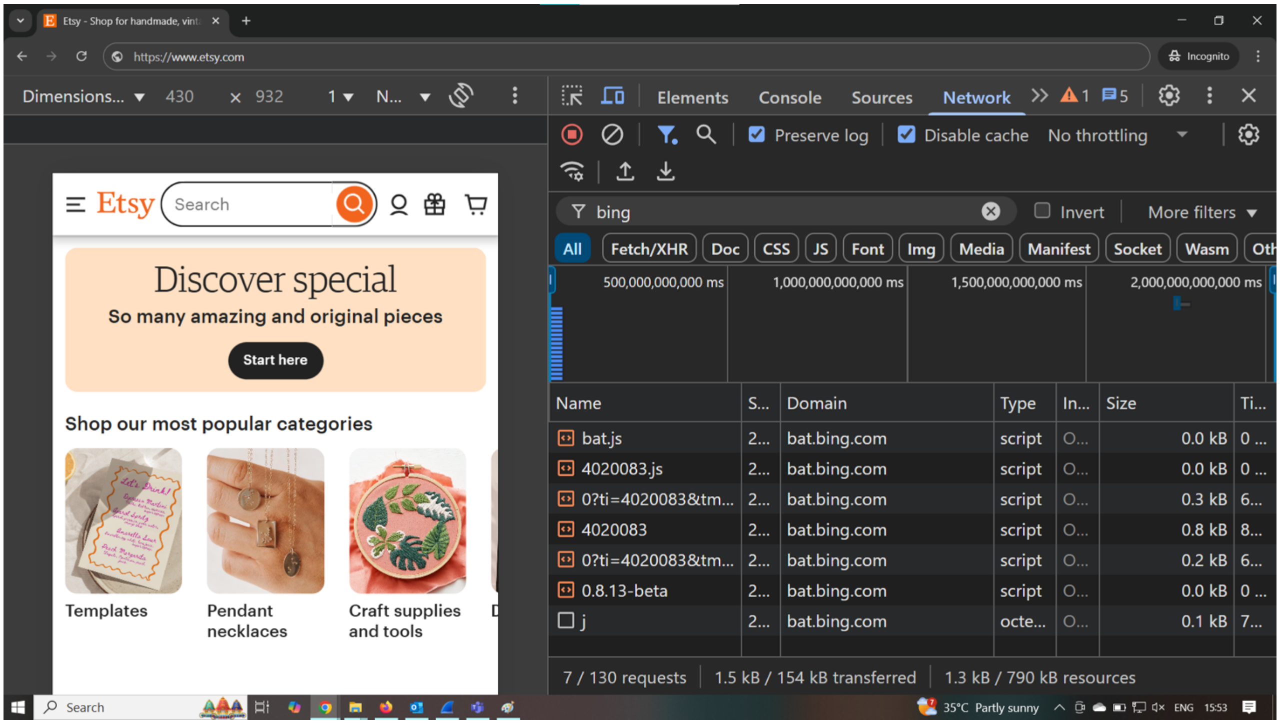
/ /

/ /

/ /

/ /

Figure 8



bing

Name	S...	Domain	Type	In...	Size	Ti...
bat.js	2...	bat.bing.com	script	O...	0.0 kB	0 ...
4020083.js	2...	bat.bing.com	script	O...	0.0 kB	0 ...
0?ti=4020083&tm...	2...	bat.bing.com	script	O...	0.3 kB	6...
4020083	2...	bat.bing.com	script	O...	0.8 kB	8...
0?ti=4020083&tm...	2...	bat.bing.com	script	O...	0.2 kB	6...
0.8.13-beta	2...	bat.bing.com	script	O...	0.0 kB	0 ...
j	2...	bat.bing.com	octe...	O...	0.1 kB	7...

7 / 130 requests | 1.5 kB / 154 kB transferred | 1.3 kB / 790 kB resources

115. ***Figure 9*** below is a screenshot of network activity on the Website, capturing DNS queries and responses for the domain bat.bing.com. This confirms that the Bing / Microsoft Ads Tracker was resolved during the user's session on the homepage. The DNS resolution occurred automatically without any user interaction, verifying that Microsoft's tracking infrastructure was silently activated as part of background communication during page load.

/ /

/ /

/ /

/ /

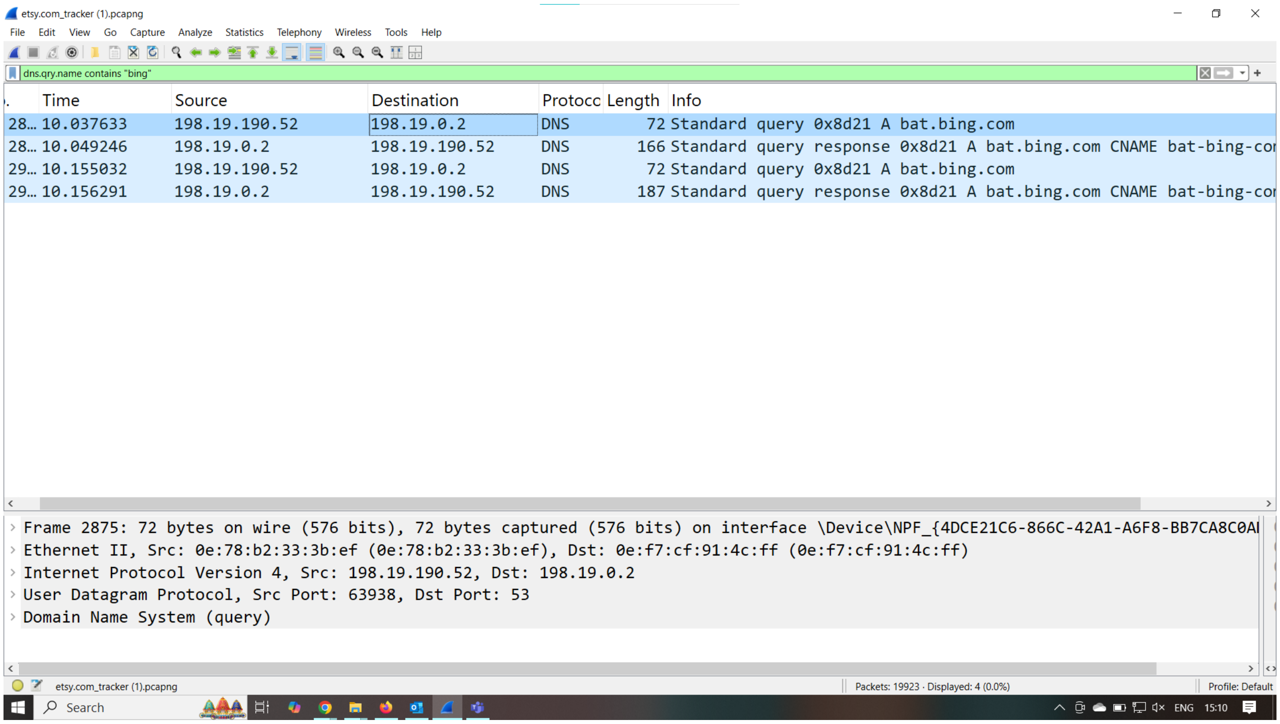
/ /

/ /

/ /

/ /

Figure 9



etsy.com_tracker (1).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains "bing"

```
.  Time       Source         Destination    Protocc Length Info
28… 10.037633 198.19.190.52  198.19.0.2     DNS         72 Standard query 0x8d21 A bat.bing.com
28… 10.049246 198.19.0.2     198.19.190.52  DNS        166 Standard query response 0x8d21 A bat.bing.com CNAME bat-bing-co
29… 10.155032 198.19.190.52  198.19.0.2     DNS         72 Standard query 0x8d21 A bat.bing.com
29… 10.156291 198.19.0.2     198.19.190.52  DNS        187 Standard query response 0x8d21 A bat.bing.com CNAME bat-bing-co
```

```
> Frame 2875: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{4DCE21C6-866C-42A1-A6F8-BB7CA8C0A
> 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: 63938, Dst Port: 53
> Domain Name System (query)
```

etsy.com_tracker (1).pcapng
Packets: 19923 · Displayed: 4 (0.0%)
Profile: Default
Search
ENG
15:10

116. 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.

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

118. 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).

119. 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.

120. 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.

121. 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.

122. 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.

5. The Trade Desk Tracker

123. The Trade Desk Tracker, typically delivered via the domain adsrvr.org, is a third-party behavioral tracking pixel operated by The Trade Desk, Inc. On the Website, this tracker is dynamically injected into users' browsers upon visiting the site. The tracker initiates a connection to The Trade Desk's servers and captures a range of data points including IP address, device type, browser version, geolocation, and unique cookie or device identifiers. These transmissions occur silently and without user interaction, confirming that user activity is being monitored in real time for purposes of behavioral profiling, identity resolution, and targeted advertising.

124. Once activated, the Trade Desk Tracker plays a central role in identity resolution by assigning users a persistent identifier that can be recognized across other websites, apps, and devices. This is accomplished through techniques such as cookie syncing and probabilistic matching, tools that allow The Trade Desk to correlate behavioral data collected on the Website with broader user profiles across the internet.

These mechanisms enable The Trade Desk to build a cohesive view of an individual's online behavior even when they are not logged in.

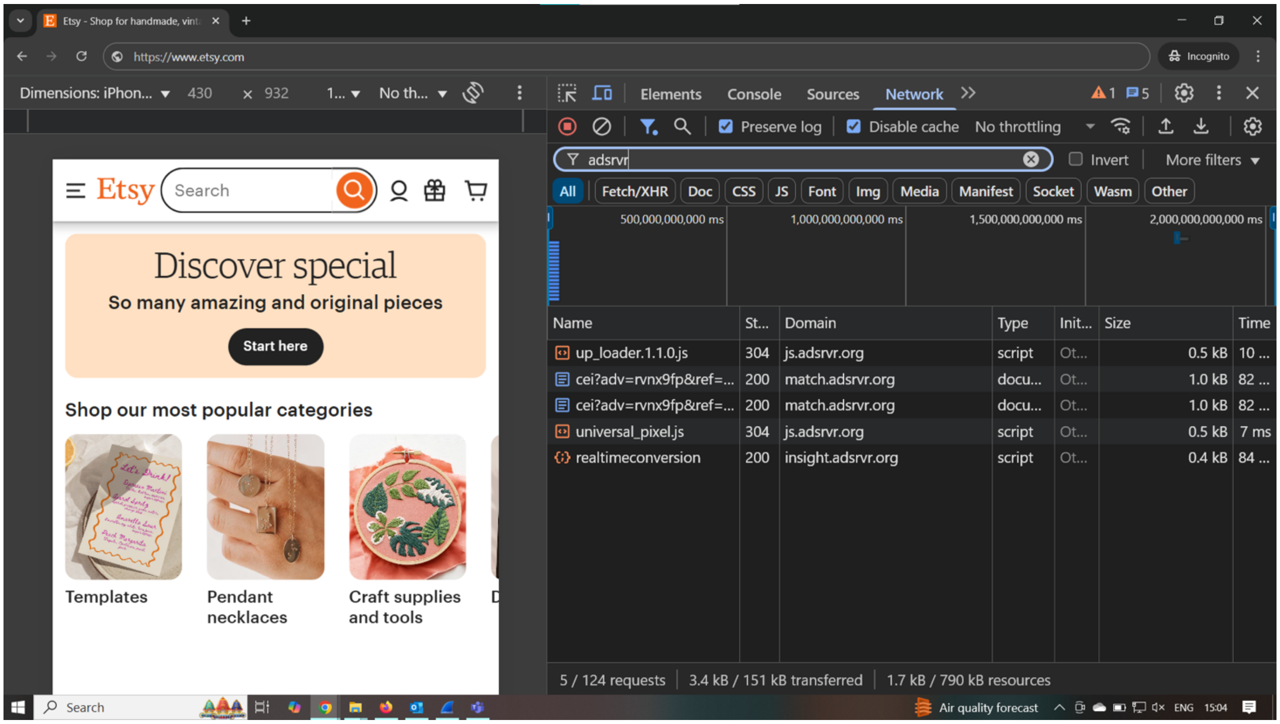
125. The Trade Desk Tracker facilitates targeted advertising by enabling ETSY to reach users who previously visited the Website, interacted with specific content, or initiated transactions. This includes retargeting individuals with personalized ads served across a broad advertising ecosystem spanning thousands of partner websites and ad exchanges. The Trade Desk's data enrichment tools allow ETSY to identify behavioral traits among its site visitors and assemble lookalike audiences composed of users who exhibit similar interests or attributes. These capabilities significantly expand ETSY's ability to re-engage high-value users and acquire new customers aligned with its marketing objectives.

126. On the Website, The Trade Desk Tracker converts user interactions into revenue-generating behavioral data by extracting real-time engagement signals and transforming them into actionable advertising segments. By tracking users across multiple touchpoints and matching them to audience categories, ETSY gains access to detailed performance analytics and the ability to optimize ad spend. The data collected feeds into a programmatic ad-buying ecosystem where advertisers compete to show personalized ads to high-value users based on the behavioral signals extracted from user interactions on ETSY's site. In this way, The Trade Desk enables ETSY to monetize user attention while facilitating profiling, ad targeting, and real-time auction-based advertising.

127. ***Figure 10*** below is a screenshot from the Website, confirming that The Trade Desk Tracker was triggered automatically upon visiting the homepage. Script and document requests were sent to domains including js.adsrvr.org, match.adsrvr.org, and insight.adsrvr.org, which are operated by The Trade Desk. These requests returned HTTP 200 and 302 status codes, confirming active communication with The Trade Desk's tracking infrastructure. This activity occurred prior to any user interaction,

verifying that The Trade Desk Tracker was actively collecting session metadata during the initial page load on the Website.

Figure 10



Name	St...	Domain	Type	Init...	Size	Time
up_loader.1.1.0.js	304	js.adsrvr.org	script	Ot...	0.5 kB	10 ...
cei?adv=rvnx9fp&ref=...	200	match.adsrvr.org	docu...	Ot...	1.0 kB	82 ...
cei?adv=rvnx9fp&ref=...	200	match.adsrvr.org	docu...	Ot...	1.0 kB	82 ...
universal_pixel.js	304	js.adsrvr.org	script	Ot...	0.5 kB	7 ms
realtimeconversion	200	insight.adsrvr.org	script	Ot...	0.4 kB	84 ...

5 / 124 requests | 3.4 kB / 151 kB transferred | 1.7 kB / 790 kB resources

128. ***Figure 11*** below is a screenshot of network activity on the Website, capturing DNS queries and responses for multiple subdomains of adsrvr.org, including js.adsrvr.org, insight.adsrvr.org, and match.adsrvr.org. These domains are controlled by The Trade Desk. The DNS activity confirms that the user's browser initiated background resolution of The Trade Desk's infrastructure during the homepage session. This activity occurred automatically and without any user interaction, verifying that the Trade Desk Tracker was operational and actively facilitating communication with a third-party server controlled by The Trade Desk.

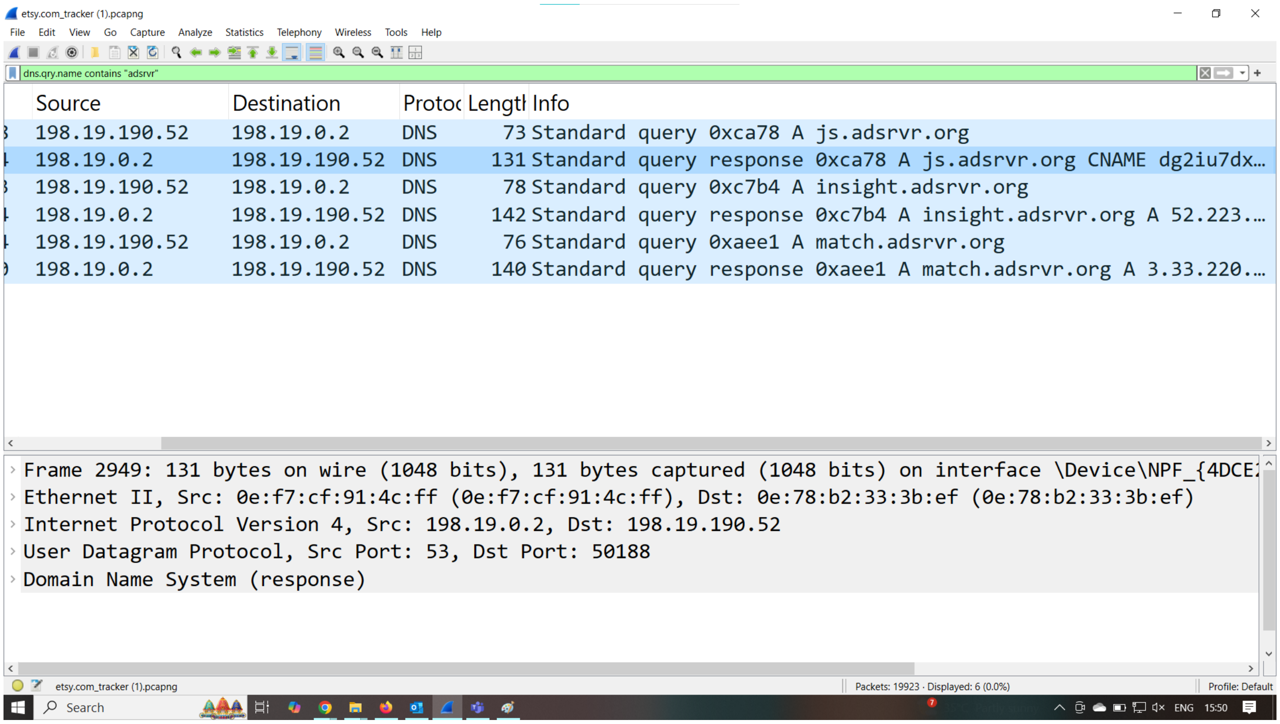
/ /

/ /

/ /

/ /

Figure 11



etsy.com_tracker (1).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains "adsrvr"

```
  Source          Destination     Protoc Lengtl Info
3 198.19.190.52   198.19.0.2      DNS       73 Standard query 0xca78 A js.adsrvr.org
4 198.19.0.2      198.19.190.52   DNS      131 Standard query response 0xca78 A js.adsrvr.org CNAME dg2iu7dx…
3 198.19.190.52   198.19.0.2      DNS       78 Standard query 0xc7b4 A insight.adsrvr.org
4 198.19.0.2      198.19.190.52   DNS      142 Standard query response 0xc7b4 A insight.adsrvr.org A 52.223.…
4 198.19.190.52   198.19.0.2      DNS       76 Standard query 0xaee1 A match.adsrvr.org
9 198.19.0.2      198.19.190.52   DNS      140 Standard query response 0xaee1 A match.adsrvr.org A 3.33.220.…
```

```
> Frame 2949: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface \Device\NPF_{4DCE
> Ethernet II, Src: 0e:f7:cf:91:4c:ff (0e:f7:cf:91:4c:ff), Dst: 0e:78:b2:33:3b:ef (0e:78:b2:33:3b:ef)
> Internet Protocol Version 4, Src: 198.19.0.2, Dst: 198.19.190.52
> User Datagram Protocol, Src Port: 53, Dst Port: 50188
> Domain Name System (response)
```

etsy.com_tracker (1).pcapng
Packets: 19923 · Displayed: 6 (0.0%)
Profile: Default
Search
ENG
15:50

129. Defendant surreptitiously installed, executed, embedded, or injected The Trade Desk Tracker onto users' browsers by deploying JavaScript code that triggers communication with The Trade Desk's tracking infrastructure. When a user visits the Website, their browser automatically executes this code, initiating outbound requests to The Trade Desk's servers and transmitting user metadata, including IP address, page URL, and unique identifiers. This transmission occurs silently and without any user action, allowing The Trade Desk to capture data about user interactions on the Website in real time.

130. The Trade Desk Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

131. The Trade Desk 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).

132. The Trade Desk 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.

133. The user does not intentionally initiate any communication with The Trade Desk; rather, the connection is automatically triggered in the background by embedded third-party code. As a result, The Trade Desk is able to silently intercept and log communication-related data generated during the user's interaction with the Website. In this way, the Trade Desk Tracker functions as a surveillance mechanism that captures third-party signaling information.

134. 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 Trade Desk Tracker on Plaintiff's and Class Members' browser or to collect or share data with The Trade Desk.

135. Consequently, The Trade Desk Tracker violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

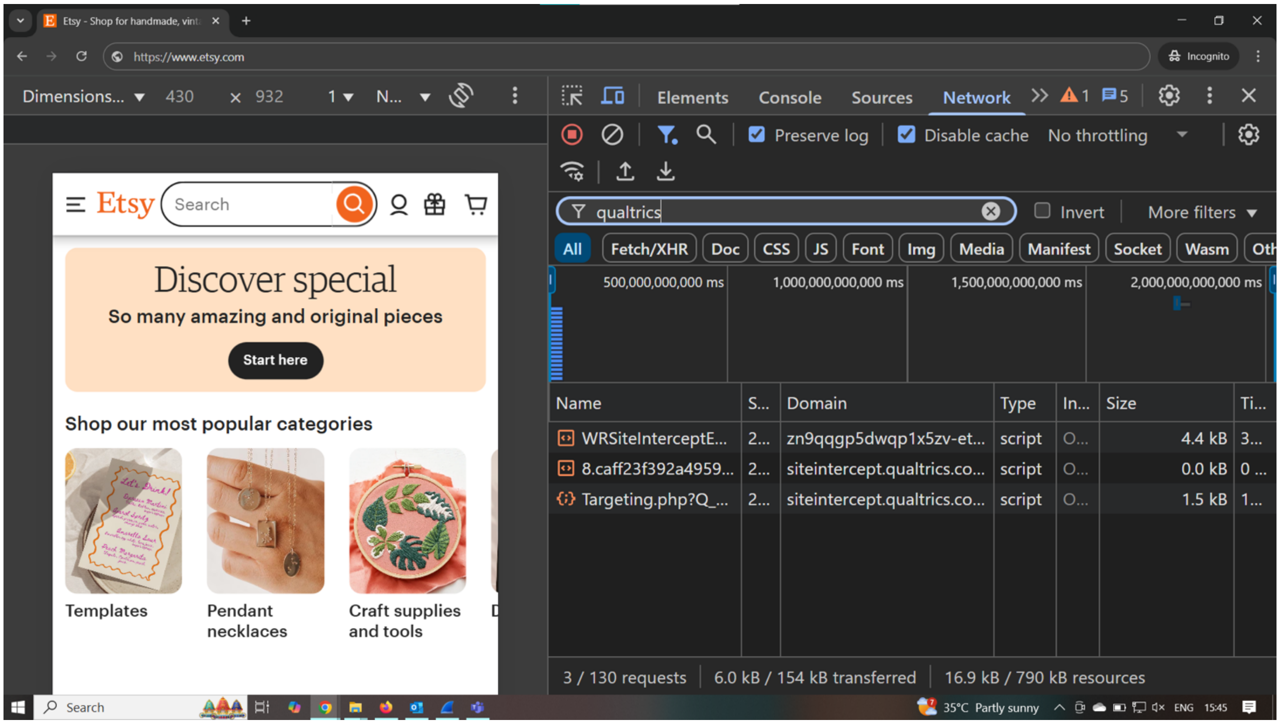
6. The Qualtrics Tracker

136. The Qualtrics Tracker is a data collection tool used to capture user behavior, session metadata, and user feedback through embedded survey scripts and event listeners. When deployed on a website, the Qualtrics Tracker can collect information such as mouse movements, page views, timestamps, device and browser attributes, IP addresses, and user interactions. On the Website, the Qualtrics Tracker was present in the session and initiated tracking behavior as soon as the site loaded.

137. By capturing this behavioral and technical data, the Qualtrics Tracker facilitates session analysis, user profiling, and real-time feedback collection. It enables ETSY to associate user interactions with demographic and behavioral attributes, which can be used for segmentation, personalization, and marketing optimization. This contributes to both identity resolution and data monetization by helping ETSY better understand and target its users.

138. ***Figure 12*** below is a screenshot from the Website, confirming that the Qualtrics Tracker was triggered automatically upon visiting the homepage. A GET request to siteintercept.qualtrics.com was initiated during the initial session and returned a 200 OK status. The request URL contains session metadata including the page URL, timestamp, and tracking parameters, confirming that the Qualtrics Tracker was actively communicating with Qualtrics's servers without any user interaction.

Figure 12



Etsy - Shop for handmade, vint

https://www.etsy.com

Dimensions... 430 × 932 1 N...

Elements Console Sources Network

☑ Preserve log ☑ Disable cache No throttling

qualtrics

□ Invert More filters

All Fetch/XHR Doc CSS JS Font Img Media Manifest Socket Wasm Oth

500,000,000,000 ms 1,000,000,000,000 ms 1,500,000,000,000 ms 2,000,000,000,000 ms

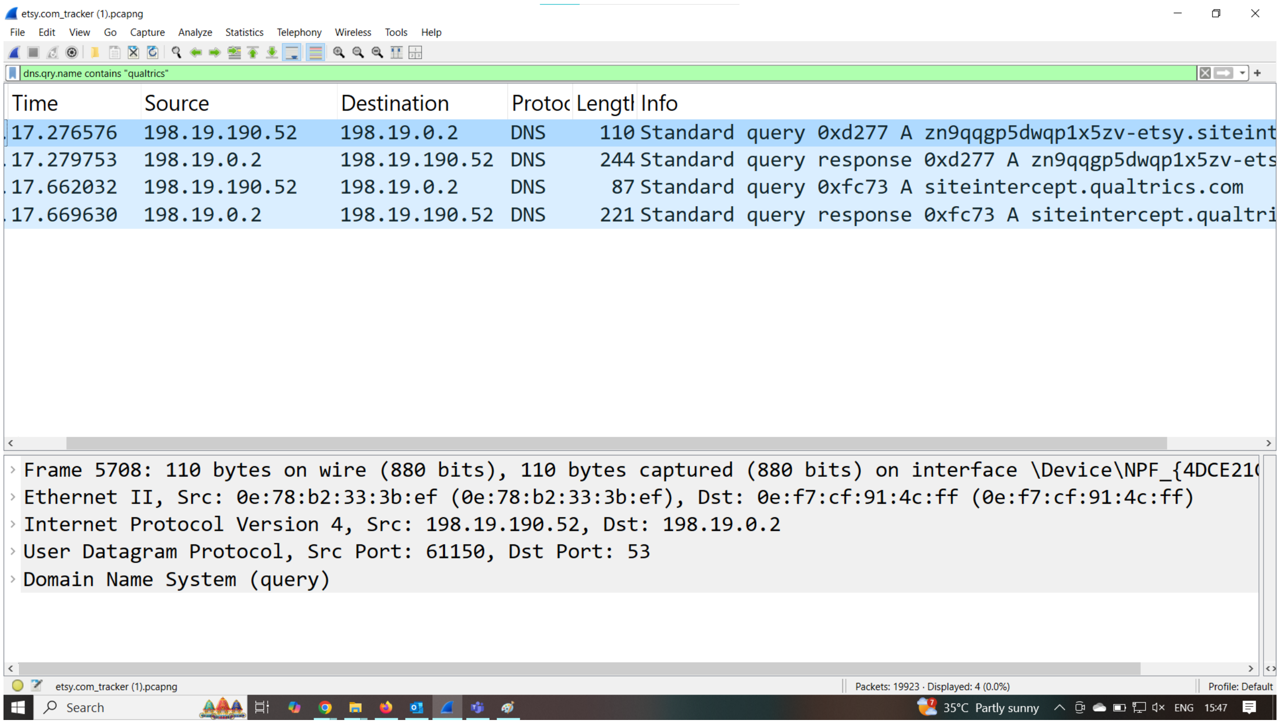
Name	S...	Domain	Type	In...	Size	Ti...
WRSiteInterceptE...	2...	zn9qqgp5dwqp1x5zv-et...	script	O...	4.4 kB	3...
8.caff23f392a4959...	2...	siteintercept.qualtrics.co...	script	O...	0.0 kB	0 ...
Targeting.php?Q_...	2...	siteintercept.qualtrics.co...	script	O...	1.5 kB	1...

3 / 130 requests | 6.0 kB / 154 kB transferred | 16.9 kB / 790 kB resources

139. ***Figure 13*** below is a screenshot of network activity on the Website, capturing a DNS query and response for siteintercept.qualtrics.com, a domain controlled by Qualtrics. This activity confirms that the user's browser initiated a resolution request for Qualtrics's tracking domain during the homepage session. The DNS request was automatically triggered without any user interaction, confirming that the Qualtrics Tracker was operational and communicating with Qualtrics's servers in the background.

/ /

Figure 13



dns.qry.name contains "qualtrics"

```
Time       Source         Destination    Protoc Lengtl Info
17.276576  198.19.190.52  198.19.0.2     DNS       110 Standard query 0xd277 A zn9qqgp5dwqp1x5zv-etsy.siteint
17.279753  198.19.0.2     198.19.190.52  DNS       244 Standard query response 0xd277 A zn9qqgp5dwqp1x5zv-ets
17.662032  198.19.190.52  198.19.0.2     DNS        87 Standard query 0xfc73 A siteintercept.qualtrics.com
17.669630  198.19.0.2     198.19.190.52  DNS       221 Standard query response 0xfc73 A siteintercept.qualtri
```

```
Frame 5708: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{4DCE21(
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: 61150, Dst Port: 53
Domain Name System (query)
```

etsy.com_tracker (1).pcapng | Packets: 19923 · Displayed: 4 (0.0%) | Profile: Default

140. Defendant surreptitiously installed, executed, or injected the Qualtrics Tracker onto users' browsers by triggering Qualtrics's JavaScript tracking code during page load. When a user visits the Website, their browser executes the script, which transmits data about the user's interactions including the user's IP address, page URL, and session metadata to Qualtrics's servers. This transmission occurs automatically and silently, without the user's awareness or interaction.

141. The Qualtrics Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

142. The Qualtrics 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).

143. The Qualtrics Tracker captures non-content signaling information such as IP addresses, URLs visited, timestamps, browser and device identifiers, and referrer data associated with electronic communications between the user and the Website. This metadata reflects addressing and routing details.

144. Qualtrics engages in user tracking and behavioral profiling, without the user's awareness or consent, by collecting and processing granular session-level data on behalf of Defendant.

145. The persistent identifiers used by Qualtrics allow it to track user behavior across sessions and contexts, enabling ETSY to build detailed user profiles and optimize marketing and engagement strategies without user awareness or consent.

146. The Qualtrics Tracker initiates a connection to Qualtrics's servers (typically at siteintercept.qualtrics.com) upon page load. This connection transmits routing and signaling metadata, including the user's IP address, user-agent string, full URL path, referrer header, and timestamp. These data points enable Qualtrics to identify the source and destination of the communication and to process user session metadata for targeting and analytics purposes. Accordingly, the Qualtrics Tracker functions as a pen register and/or trap and trace device and/or process.

147. 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' consent to install the Qualtrics Tracker or to collect or share data with Qualtrics.

148. Consequently, the Defendant's secret installation of the Qualtrics Tracker on the Website violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

7. The Podscribe Tracker

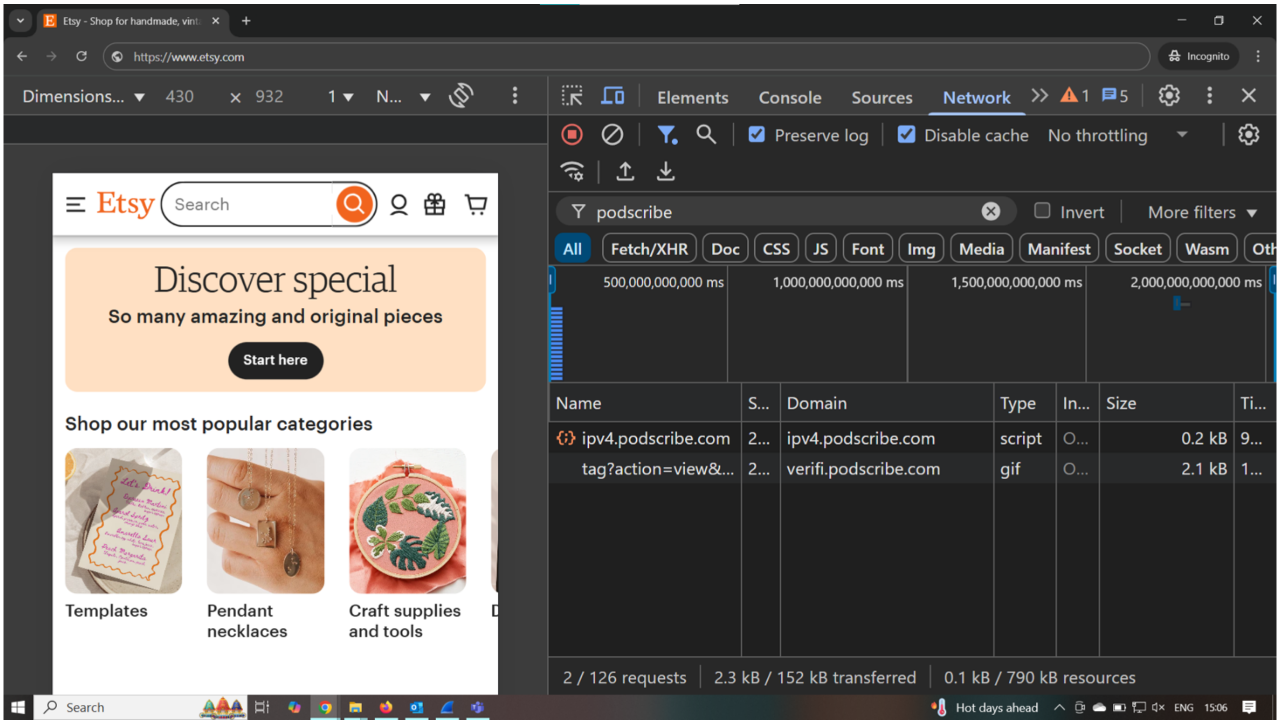
149. The Podscribe Tracker is a session-level tracking and data collection tool operated by Podscribe, a podcast analytics and attribution company. When deployed on the website, the Podscribe Tracker captures visitor metadata, including IP address, page URL, browser and device information, and session timing. On the Website, the Podscribe Tracker was present during the session and initiated communications with Podscribe's infrastructure as soon as the site loaded, enabling ETSY to analyze user behavior and measure advertising attribution without the user's knowledge or

engagement.

150. The Podscribe Tracker enables session-level tracking by transmitting metadata to Podscribe's servers immediately upon page load. The data collected includes user-agent strings, timestamps, referrer headers, and unique identifiers that can be used to analyze user activity and evaluate advertising performance. Podscribe's tracking infrastructure allows ETSY to correlate this metadata with podcast-related user engagement metrics for attribution, profiling, and marketing optimization.

151. ***Figure 14*** below is a screenshot from the Website, confirming that the Podscribe Tracker was triggered automatically upon visiting the homepage. A GET request to the domain verifi.podscribe.com returned a 200 OK response and included session metadata. This request was initiated without any user interaction, confirming that the Podscribe Tracker was actively transmitting user data to Podscribe's servers during the initial page load.

Figure 14



☑ Preserve log ☑ Disable cache No throttling

Filter: podscribe

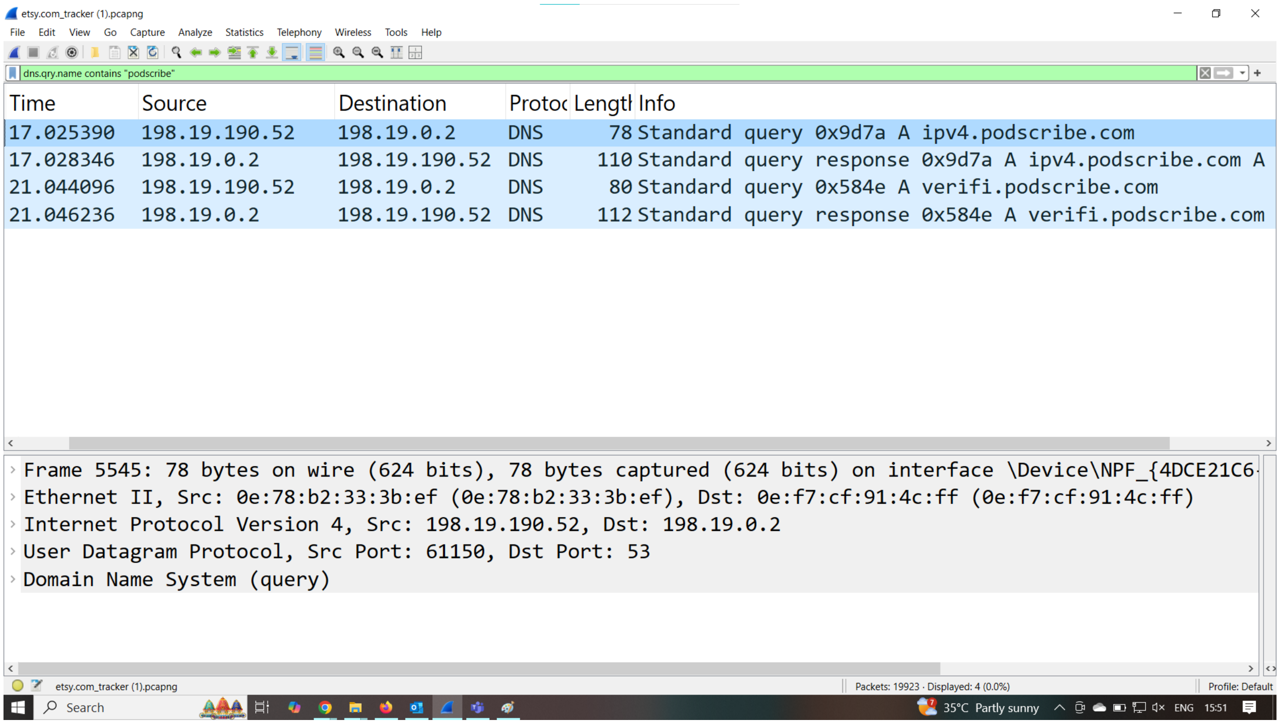
Name	S...	Domain	Type	In...	Size	Ti...
ipv4.podscribe.com	2...	ipv4.podscribe.com	script	O...	0.2 kB	9...
tag?action=view&...	2...	verifi.podscribe.com	gif	O...	2.1 kB	1...

2 / 126 requests | 2.3 kB / 152 kB transferred | 0.1 kB / 790 kB resources

152. ***Figure 15*** below is a screenshot of network activity on the Website, which captures a DNS query and corresponding response for verifi.podscribe.com, a

domain controlled by Podscribe. This activity confirms that the user's browser initiated a request to resolve Podscribe's tracking domain during the homepage session. The DNS resolution occurred automatically in the background, without any user interaction, and demonstrates that the Podscribe Tracker was active and facilitating communication with Podscribe's servers.

Figure 15



etsy.com_tracker (1).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns.qry.name contains "podscribe"

Time       Source          Destination     Protoc Lengtl Info
17.025390  198.19.190.52   198.19.0.2      DNS       78 Standard query 0x9d7a A ipv4.podscribe.com
17.028346  198.19.0.2      198.19.190.52   DNS      110 Standard query response 0x9d7a A ipv4.podscribe.com A
21.044096  198.19.190.52   198.19.0.2      DNS       80 Standard query 0x584e A verifi.podscribe.com
21.046236  198.19.0.2      198.19.190.52   DNS      112 Standard query response 0x584e A verifi.podscribe.com

> Frame 5545: 78 bytes on wire (624 bits), 78 bytes captured (624 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: 61150, Dst Port: 53
> Domain Name System (query)

etsy.com_tracker (1).pcapng    Packets: 19923 · Displayed: 4 (0.0%)    Profile: Default
```

153. Defendant surreptitiously installed, executed, or injected the Podscribe Tracker onto users' browsers by deploying JavaScript tracking code that initiated outbound requests to Podscribe's servers. When a user visits the Website, the browser executes the Podscribe script, which collects user interaction metadata including the user's IP address, page URL, session details, and referrer and transmits it to Podscribe's servers in real time, without the user's awareness or consent.

154. The Podscribe Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

155. The Podscribe 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).

156. The Podscribe Tracker captures non-content signaling information such as IP addresses, visited URLs, timestamps, and referrer data associated with electronic communications. These data points reveal routing and addressing details and allow ETSY and Podscribe to monitor user sessions for tracking and attribution purposes.

157. Podscribe engages in user tracking and profiling on behalf of ETSY by processing session metadata and associating it with podcast-related marketing activities. The tracking occurs without any user interaction, knowledge, or consent and contributes to ETSY's behavioral profiling and advertising strategy.

158. The Podscribe Tracker initiates a connection to Podscribe's infrastructure immediately upon page load. The transmission includes routing and signaling metadata such as IP address, user-agent, full URL, and timestamps, which qualify as pen register and trap and trace data under CIPA.

159. 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' consent to install the Podscribe Tracker or to collect or share data with Podscribe.

160. Consequently, the Defendant's secret installation of the Podscribe Tracker on the Website violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

VI. <u>CLASS ALLEGATIONS</u>

161. 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.

/ /

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

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

- Whether Defendant installed, executed, embedded or injected the Trackers on the Website;
- Whether the Trackers are each a pen register and/or trap and trace device as defined by law;
- Whether Plaintiff and Class Members are subject to same tracking policies and practices;
- Whether Plaintiff and Class Members are entitled to statutory penalties;
- Whether Class Members are entitled to injunctive relief;
- Whether Class Members are entitled to disgorgement of data unlawfully obtained;
- Whether the Defendant's conduct violates CIPA; and
- Whether the Defendant’s conduct constitutes an unlawful, misleading, deceptive or fraudulent business practice.

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

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

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.

166. **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. <u>FIRST CAUSE OF ACTION</u>

Violations of Cal. Penal Code § 638.51

By Plaintiff and the Class Members Against All Defendants

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

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

169. 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.

170. 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

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

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

173. 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.

174. 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).

175. 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.

176. 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.

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

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

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

IX. <u>**PRAYER FOR RELIEF**</u>

WHEREFORE, Plaintiff prays for the following:

1. An order certifying the Class, naming Plaintiff as Class representative, and naming Plaintiff's attorneys as Class counsel;
2. An order declaring that Defendant's conduct violates CIPA and Business & Professions Code § 17200;
3. An order of judgment in favor of Plaintiff and the Class against 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 3, 2025 **NATHAN & ASSOCIATES, APC**

By: /s/ Reuben D. Nathan
Reuben D. Nathan, Esq.
Attorneys for Plaintiff