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, JEFFREY SCRUGGS

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JEFFREY SCRUGGS, on behalf of himself and all similarly situated persons,

Plaintiff,

v.

TICKETMASTER L.L.C., a Virginia limited liability company,

Defendant.

Case No:

CLASS ACTION COMPLAINT

1) Cal. Penal Code § 638.51
2) Cal. Constitution Art. I § 1
3) Cal. Bus. & Prof. Code § 17200, *et seq.*
4) Intrusion Upon Seclusion
5) Unjust Enrichment

Plaintiff JEFFREY SCRUGGS ("Plaintiff") files this class action complaint on behalf of himself and all others similarly situated (the "Class Members") against Defendant TICKETMASTER L.L.C., a Virginia limited liability company ("Defendant" or "TICKETMASTER"). Plaintiff brings this action based upon personal knowledge of the facts pertaining to himself, and on information and belief as to all others, by and through the investigation of undersigned counsel.

I. NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all California residents who have accessed and used www.ticketmaster.com the "Website"), a website that Defendant provides for public access and use.

2. Defendant surreptitiously installs and operates tracking software on the Website without providing users with adequate notice or obtaining their informed consent. The software is intentionally deployed to accomplish Defendant's commercial objectives, including identity resolution, targeted advertising, and the monetization of consumer data.

3. To achieve these goals, Defendant enables third-party technologies on its Website that function as unlawful pen registers and/or trap-and-trace devices or processes. These technologies automatically capture and transmit non-content dialing, routing, addressing, and signaling information including Internet Protocol (IP) addresses, page URLs, referrer headers, timestamps, session identifiers, and device or browser identifiers to third-party servers in real time during users' interactions with the Website. Defendant deploys these technologies without judicial authorization and without obtaining Plaintiff's or Class Members' consent, in violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 638.51.

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 causes the user's browser to transmit data to third-party servers, including page-view events, page URLs, referrer headers, session-level identifiers, network-level IP addressing information, browser and device characteristics, and related navigation metadata.

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

- Google Trackers (Analytics, Ads, Tag Manager, DoubleClick)
- Facebook Tracker
- TikTok Tracker
- Microsoft Bing 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, which go beyond Defendant's direct needs, for their own financial gain. The above-listed trackers are referred to herein collectively as the "Trackers."

8. The Trackers are operated by distinct third-party entities, including Google LLC (as to Google Tag Manager, Google Analytics, and Google Ads/DoubleClick), Meta Platforms, Inc. (as to the Facebook/Meta Pixel), TikTok Inc. (as to the TikTok Tracker), and Microsoft Corporation (as to the Microsoft Bing/UET Tracker) (collectively, the "Third Parties"). Defendant knowingly embeds and enables these Trackers on the Website and configures them to execute automatically within users' browsers upon page load and navigation. Through this configuration, Defendant causes users' browsers to transmit non-content Dialing, Routing, Addressing, and Signaling ("DRAS") information—including page URLs, referrer paths, timestamps, session- and browser-level identifiers, device and browser characteristics, and related network metadata—to servers controlled by the Third Parties. These transmissions occur as part of advertising measurement, attribution, analytics, and identity-linked tracking

workflows and are not necessary to deliver or display the Website's core content or functionality. Defendant's deployment of these Trackers is deliberate and coordinated, reflecting affirmative design choices to permit third-party acquisition of DRAS information during ordinary use of the Website.

9. On information and belief, Defendant's Website is further equipped with additional third-party tracking and advertising technologies operated by Pinterest, Inc. (as to the Pinterest Tag), Snap Inc. (as to the Snapchat Pixel), and Comscore, Inc., a registered California data broker (as to Comscore measurement and analytics technologies). These third-party technologies execute within users' browsers as part of the Website's ordinary operation and are designed to collect, receive, and process non-content Dialing, Routing, Addressing, and Signaling ("DRAS") information, including IP addresses, page URLs, referrer paths, timestamps, session-level identifiers, and device or browser characteristics. The information transmitted through these technologies supports functions including advertising measurement, audience segmentation, behavioral analytics, and cross-site tracking. Defendant deploys these third-party technologies without prior user consent and without any court authorization.

10. Through the Trackers, the Third Parties collect a wide range of dialing, routing, addressing, and signaling information from users' browsers and devices without user consent. This information includes network-level IP addressing information; page URLs and referrer headers; browser and device type; operating system and platform information; language and locale settings; persistent and session-level identifiers (including cookies and advertising or deduplication identifiers); and other navigation-related metadata transmitted during page load and site interaction. The Trackers also enable the derivation of approximate geographic location from IP addressing information. Collectively, this data ("User Information") is used for behavioral profiling, advertising measurement and attribution, personalization, audience segmentation, and identity-linked tracking. Defendant deploys the Trackers and permits the collection and

commercial use of User Information in coordination with the Third Parties operating them to support targeted marketing and advertising that monetizes the Website.

11. The third-party tracking code executed contemporaneously with each page load and navigation event initiated by Plaintiff's browser. As the browser initiated each HTTP request to retrieve Website content, embedded scripts automatically caused the transmission of dialing, routing, addressing, and signaling information to remote third-party endpoints during the page-load process itself, before the requested page finished rendering and without any user interaction or authorization.

12. Because the Trackers record and transmit DRAS information, including network-level IP addressing information, full page URLs, referrer headers, persistent and session-level identifiers, and browser and device characteristics, they operate as "pen registers" and/or "trap and trace devices" within the meaning of California Penal Code §§ 638.50, 638.51. These technologies function as automated processes that collect routing and addressing metadata for commercial purposes during page load and navigation without the user's consent. Courts have recognized that the unauthorized use of such tracking technologies to capture routing, addressing, and signaling information falls within the scope of CIPA's prohibitions. *See, e.g., Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023).

13. The privacy intrusion alleged herein is heightened by the nature of the third-party entities that operate the Trackers embedded on Defendant's Website and receive Plaintiff's and Class Members' Dialing, Routing, Addressing, and Signaling ("DRAS") information. As alleged above, Defendant causes users' browsers to transmit network-level IP addressing information, persistent and session-level identifiers, page URLs, referrer paths, timestamps, and related signaling metadata to third parties including Google LLC, Meta Platforms, Inc., TikTok Inc., Microsoft Corporation (Bing), Pinterest, Inc., Snap Inc., and Comscore, Inc. These entities operate tracking, analytics, and advertising technologies that are designed to receive and process addressing and signaling data generated by users' interactions with websites. By enabling and

configuring these Trackers, Defendant permits third parties to collect and process users' routing and addressing metadata associated with navigation of Defendant's Website, without Plaintiff's consent and without any court authorization, in violation of California Penal Code § 638.51.

14. Plaintiff and the Class Members did not consent to the installation, execution, embedding, or injection of the Trackers on their devices. The Website did not display any consent banner, pop-up, cookie notice, or other authorization mechanism requesting permission before deploying pen-register or trap-and-trace devices or processes. Defendant did not obtain express prior consent for the collection and transmission of dialing, routing, addressing, and signaling information for advertising, analytics, or monetization purposes. General statements contained in a privacy policy accessible only through non-blocking hyperlinks do not constitute express prior consent under California law.

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

II. PARTIES

16. Plaintiff JEFFREY SCRUGGS is a California citizen residing in Solano County, CA and has an intent to remain there. Plaintiff was in California when he visited the Website, which occurred during the class period including but not limited to on December 4, 2025. The allegations set forth herein are based on the Website as configured when Plaintiff visited it.

17. TICKETMASTER, L.L.C. is a Virginia limited liability company that owns, operates, and/or controls the Website, an online platform through which TICKETMASTER offers goods and services to consumers.

18. TICKETMASTER is a technology company that operates an online ticketing platform for live events, including concerts, sports, theater, and other entertainment events. TICKETMASTER is organized under the laws of the State of Virginia and maintains its principal executive offices in Beverly Hills, California.

Through its Website and related digital platforms, TICKETMASTER facilitates the discovery, purchase, and distribution of event tickets to consumers in California.

19. TICKETMASTER conducts business nationwide and engages in product development, marketing, and commercial operations centered on its digital ticketing platform. TICKETMASTER's business activities include operating an online marketplace through which users browse event offerings, review ticket availability and pricing, and complete ticket purchases using web-based interfaces.

20. The Website, including the mobile site, serves as a core component of TICKETMASTER's digital presence. The Website provides users with access to event listings in California, ticket availability and pricing information for California events, search and discovery tools for events in California, promotional content, and customer-service resources, and functions as the primary consumer-facing platform through which California users browse and purchase event tickets. The Website is integrated into Ticketmaster's broader digital infrastructure and employs web-based technologies that operate in connection with page loads, navigation, and user interaction.

III. JURISDICTION AND VENUE

21. 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.

22. TICKETMASTER is subject to general personal jurisdiction in California because it is headquartered in this State. Ticketmaster's principal place of business is located at 9348 Civic Center Drive in Beverly Hills, rendering it "at home" in this forum for purposes of general jurisdiction. As a result, Ticketmaster is subject to the jurisdiction of California courts for all claims asserted in this action.

23. Venue is proper in the Central District of California pursuant to 28 U.S.C. § 1391(b) because (1) Defendant maintains its primary place of business in this District;

(2) Defendant regularly transacts business in this District and is subject to personal jurisdiction here; and (3) a substantial part of the events or omissions giving rise to the claims occurred within this District.

IV. GENERAL ALLEGATIONS

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

24. 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 e65+xercise of personal liberties and cannot be tolerated in a free and civilized society" (Cal. Penal Code § 630).

25. 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)).

26. 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)).

27. Conversely, a "trap and trace device" is a device or process that 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)).

/ / /

/ / /

28. In practical terms, a pen register is a device or process that records outgoing dialing information, while a trap and trace device is a device or process that records incoming dialing information.

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

30. 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.

31. 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.

32. 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 (N.D. Cal. Sep. 26, 2013); *see also, e.g.*, *Shah v. Fandom, Inc*, 754 F. Supp. 3d 924, 930 (N.D. Cal. 2024) (finding trackers similar to those at issue here were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educ. Sys. Inc.* 742F. Supp. 3d 1072, 1076 (C.D. Cal. 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and 638.51."); *Greenley,* supra, *at* 1050 (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v. Assurance IQ, LLC,* 2022 WL 1744107,

at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications. 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 (N.D. Cal. Aug. 12, 2016).

33. 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).)

34. 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).)

35. 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"*

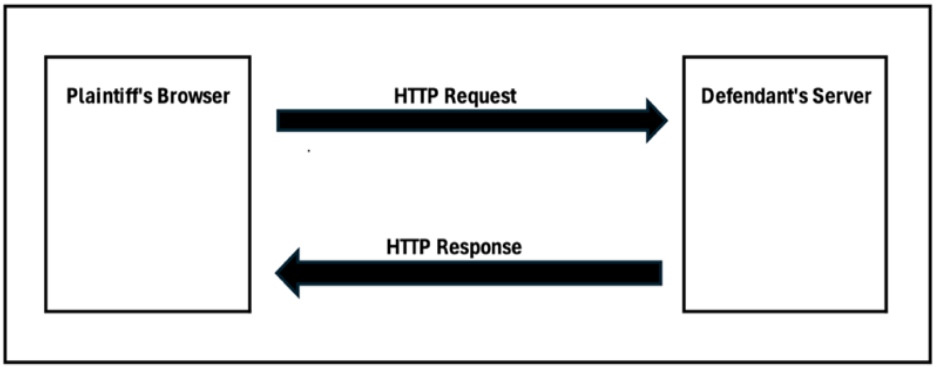
36. When the Plaintiff and Class Members accessed the Website, their browsers initiated an HTTP or HTTPS request or "GET" request to Defendant's web server, which hosts the content and functionality of the site. In response, the server transmitted an HTTP response containing the necessary resources, 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. The server's instructions include how to properly display the Website, *e.g.* what images to load, what text should appear, or what music should play.

/ / /

37. In addition, the server's instructions included client-side scripts that initiate communication with third-party services for analytics, marketing, and tracking purposes. The instructions cause the Trackers to be installed on a user's browser. The Trackers then cause the browser to send identifying information—including the user's IP address and User Information to the Third Parties. These Third Parties, through their Trackers, also set a cookie on Website users' browsers, which sends a unique identifier to these Third Parties that allows them to track users on the Website over multiple visits and across the Internet.

38. A general diagram of this process is pictured at Figure 1, which explains how Defendant's Website transmits instructions back to users' browsers in response to HTTP requests.

Figure 1:



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

40. 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 by user interactions with the Website and are used to transmit behavioral data and Device Metadata, including information such as page views, click events, session duration, and identifying browser characteristics.

41. Plaintiff and Class Members did not provide their prior consent to Defendant to install the Trackers on their browsers or use the Trackers. Nor did Defendant obtain a court order before installing or using the Trackers.

42. An 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). The traditional format of IP addresses is called IPv4, and it has a finite amount of combinations and thus is limited to approximately 4.3 billion addresses. Because this proved to be insufficient as the Internet grew, IPv6 was introduced. IPv6 offers a vastly larger address space with 340 undecillion possible addresses. While IPv6 adoption has been increasing, many networks still rely on IPv4.[1]

43. Much like a telephone number, an IP address guides or routes an intentional communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential for identifying a device on the internet or within a local network, facilitating smooth communication between devices. IP addresses can be used via external geolocation services to infer a user's general location, including state, city, approximate latitude and longitude, and in some cases, ZIP code.

44. Public IP addresses are globally unique identifiers assigned by Internet Service Providers (ISPs) that allow devices to communicate directly over the Internet.

[1] *See, e.g.*, *What is the Internet Protocol*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/internet-protocol/; Stefano Gridelli, *What is an RFC1918 Address?*, NETBEEZ (Jan. 22, 2020), https://netbeez.net/blog/rfc1918/.

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.

45. Public IP addresses can be used to determine the approximate physical location of a device. For example, services like iplocation.io, use databases that map IP addresses to geographic areas, often providing information about the country, city, approximate latitude and longitude coordinates, or even the internet service provider associated with the public IP. This geolocation capability is leveraged by online advertising and user identification services.

46. In contrast, private IP addresses are used within internal networks and are not routable on the public Internet. The Internet Assigned Numbers Authority ("IANA") reserves specific ranges of numbers to be exclusively used for private IP addresses (*e.g.*, 172.16.0.0 through 172.31.255.255). They are isolated from the global Internet and can be reused across different networks without conflict. For example, a home network in New York and an office network in Tokyo can both use the same private IP address (*e.g.*, 192.168.1.1) for their routers without conflict.

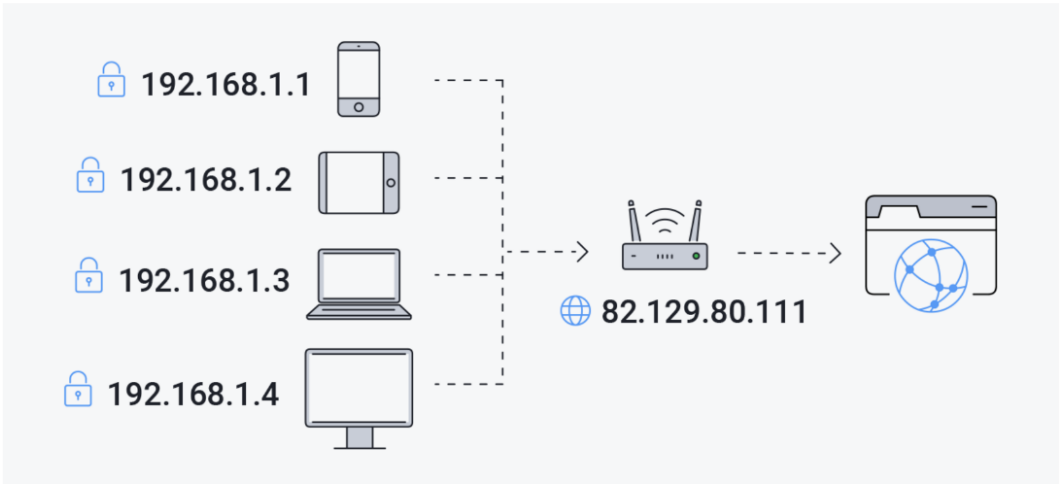
47. The distinction between a public and private IP address is fundamental to the architecture of modern networks. Public IP addresses facilitate global communication, while private IP addresses conserve the finite amount of combinations to make an IP address through local network communication. And crucially, a private IP address does not divulge a user's geolocation, whereas a public IP address does and is thus extensively used in advertising.

48. An analogy is useful. A public IP address is like the number for a landline telephone for a household. A private IP address is like each handset that is connected to that landline number (*e.g.*, "Handset #1," "Handset #2"). Alot can be gleaned from knowing the phone number who is making the call, while knowing Handset #1 versus Handset #2 is making a call provides additional information.

/ / /

49. The same is true of IP addresses. The public IP address divulges the approximate location of the user that is connecting to the Internet and the router directing those communications (presumably the user's house or workplace), and it is the means through which the user actually communicates with the website and the Internet at large. The private IP address then distinguishes between the devices accessing the same public IP address.[2]

Figure 2:



Each device on a network has a private IP address, and the router has a public IP address to communicate with the rest of the internet.

50. Thus, the differences between public and private IP addresses are as follows:[3]

/ / /

/ / /

[2] While the Trackers do not collect private IP addresses, as discussed below, the Trackers also collect Device Metadata, which distinguishes between devices accessing the same public IP address. So, by installing the Trackers on Website users' browsers, Defendant allows third parties to collect information that is analogous to a telephone number (the public IP address) and the specific handset that is making the call (the "Device Metadata").

[3] WHAT'S THE DIFFERENCE BETWEEN A PUBLIC AND PRIVATE IP ADDRESS?, AVIRA (Jan. 31, 2024), https://www.avira.com/en/blog/public-vs-private-ip-address.

Figure 3:

Category	Private IP address	Public IP address
Scope	The private IP address only has a local scope in your own network.	The public IP address's scope is global.
Communication	It is used so devices within a network can communicate with each other.	It allows access to the internet and is used for communication outside of your own network.
Uniqueness	It's an address from a smaller range that's used by other devices in other local networks.	It's a unique address that's not used by other devices on the internet.
Provider	The router assigns a private IP address to a specific device on the local network.	The internet service provider assigns the public IP address.
Range	Private IP address ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255	Any IP address that isn't within a private IP address range.

51. A public IP address is therefore "routing, addressing, or signaling information." 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.

52. As "routing, addressing, or signaling information," a public IP address is indispensable for maintaining seamless and efficient connection 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.

53. A public IP address is "addressing" information because it determines the general geographic coordinates of the user who is accessing a website.

/ / /

54. A public IP address is "routing" or "signaling" information because it is sending or directing the user's communication from the router in their home or work to the website they are communicating with, and ensuring that "emails, websites, streaming content, and other data reaches you correctly."[4]

55. Through a public IP address, a device's state, city, zip code, and approximate latitude and longitude can be determined. Thus, knowing a user's public IP address and therefore geographical location "provide[s] a level of specificity previously unfound in marketing."[5]

56. A public IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[6] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests."[7] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[8] because "[c]ompanies can use an IP address … to personally identify individuals."[9]

57. In fact, a public IP address is a common identifier used for "geomarketing," which is "the practice of using location data to identify and serve marketing messages to a highly-targeted audience. Essentially, geomarketing allows [websites] to better serve [their] audience by giving [them] an inside look into where they are, where they have been, and what kinds of products or services will appeal to their needs."[10] For example,

---

[4] Anthony Freda, *Private IP vs Public IP: What's the Difference?*, AVG (June 4, 2021), https://www.avg.com/en/signal/public-vs-private-ip-address.

[5] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[6] *Location-Based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/.

[7] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://tinyurl.com/c2ne77ua.

[8] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[9] Trey Titone, *The Future Of IP Address As An Advertising Identifier*, AD TECH EXPLAINED (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.

[10] *See, e.g.*, *The Essential Guide to Geomarketing: Strategies, Tips & More*, DEEP SYNC (Nov. 20, 2023), https://deepsync.com/geomarketing/.

for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.[11]

58. "IP targeting is a highly effective digital advertising technique that allows you to deliver ads to specific physical addresses based on their internet protocol (IP) address. IP targeting technology works by matching physical addresses to IP addresses, allowing advertisers to serve ads to specific households or businesses based on their location."[12]

59. "IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This means that advertisers can deliver highly targeted ads to specific households or businesses, rather than relying on more general demographics or behavioral data."[13]

60. In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's public IP address because it "can be more cost-effective than other forms of advertising."[14] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[15]

61. In addition, "IP address targeting can help businesses to improve their overall marketing strategy."[16] "By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts."[17]

---

[11] *See, e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns.

[12] *IP Targeting*, SAVANT DSP, https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB.

[13] *Id.*

[14] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[15] *Id.*

[16] *Id.*

[17] *Id.*

62. The collection of IP addresses here is particularly invasive here: As a report from NATO found:

> [a] data broker may receive information about a[] [website] user, including his … IP address. The user then opens the [website] while his phone is connected to his home Wi-Fi network. When this happens, the data broker can use the IP address of the home network to identify the user's home, and append this to the unique profile it is compiling about the user. If the user has a computer connected to the same network, this computer will have the same IP address. The data broker can then use the IP address to connect the computer to the same user, and identify that user when their IP address makes requests on other publisher pages within their ad network. Now the data broker knows that the same individual is using both the phone and the computer, which allows it to track behaviour across devices and target the user and their devices with ads on different networks.[18]

63. In other words, not only does the collection of IP addresses by the Third Parties cause harm in and of itself, data brokers use IP addresses to identify users, append the IP address to a unique profile containing even more information about the user, attach specific IP addresses to comprehensive user profiles, and track Plaintiff and Class Members across the Internet using their IP addresses, compiling vast reams of other personal information in the process.

64. For these reasons, under Europe's General Data Protection Regulation, IP addresses are considered "personal data, as they can potentially be used to identify an individual."[19]

/ / /

[18] HENRIK TWETMAN & GUNDARS BERGMANIS-KORATS, NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, DATA BROKERS AND SECURITY at 11 (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[19] IS AN IP ADDRESS PERSONAL DATA?, CONVESIO, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/; *see also* WHAT IS PERSONAL DATA?, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

65. When companies build their websites, they install or integrate various third-party scripts into the code of the website in order to collect data from users or perform other functions.[20]

66. Often times, third-party scripts are installed on websites "for advertising purposes."[21]

67. Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time."[22]

68. Defendant has long incorporated the Trackers' code into the code of its Website, including when Plaintiff and Class Members visited the Website. Thus, when Plaintiff visited the Website, the Website caused the Trackers to be installed on Plaintiff's and other users' browsers.

69. As described below, when a user visits the Website, the Website's code as programmed by Defendant installs the Trackers onto the user's browser. This allows the Third Parties through their respective Trackers to collect Plaintiff's and Class Members' IP addresses, Device Metadata, and User Information, and pervasively track them across the Internet.

70. 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.

---

[20] *See Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ ("Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user's visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user's browsing history to other companies…").

[21] *Id.*

[22] *Id.*

71. Defendant and the Third Parties then use the public IP addresses, Device Metadata, User Information, and other information of Website visitors that are collected and set by the Trackers, including those of Plaintiff and Class Members, to deanonymize Plaintiff and Class Members, serve hyper-targeted advertisements, and unjustly enrich themselves through this improperly collected information. 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.

72. At no time prior to the installation and use of the Trackers on Plaintiff's and Class Members's browsers, or prior to the use of the Trackers, did Defendant procure Plaintiff's and Class Members's consent for such conduct. Nor did Defendant obtain a court order to install or use the Trackers.

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

73. 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. These transmissions occurred silently, automatically, and without any visual indication to Plaintiff. No disclosure, banner, or mechanism alerted Plaintiff that her device would serve as a communication channel to multiple unrelated advertising and identity-resolution vendors.

74. The third-party transmissions were triggered the moment Plaintiff's browser attempted to load each page, duplicating Plaintiff's outgoing GET and POST requests and routing those signals to multiple advertising and identity-resolution endpoints before the requested pages finished loading or became visible on her device.

75. The Trackers also causes additional data points to be sent from Plaintiff's and Class Members' browser to the Third Parties, which are meant to uniquely identify users across sessions and devices. In addition to the public IP address, key elements include the user-agent string (browser, operating system, and device type) and device capabilities such as supported image formats and compression methods. Persistent identifiers like the PUID, GUID, UID, PSVID, and User-Agent ensure users can be tracked even after clearing standard session data like cookies. Advanced methods like fingerprinting and server-side matching remain unaffected by cookie deletion. Combined, these elements form a detailed, unique fingerprint that allows for cross-site tracking and behavioral profiling.

76. 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.

77. 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.

78. 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).

79. 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.

80. The Trackers provide analytics and marketing services to Defendant using the data collected from visitors to the Website when they visited the Website and from when they visited other websites that included the pen register and trap and trace devices.

81. 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.

82. These transmissions were not abstract or speculative, but occurred in connection with specific, observable actions taken by Plaintiff on the Website. For example, when Plaintiff accessed the homepage and navigated to individual event listing and ticket pages, his browser generated outbound network requests associated with those page loads and navigational steps, transmitting page URLs, referrer paths, timestamps, and browser and device metadata to third-party servers automatically as part of rendering

the Website. The Specific Allegations section below identifies concrete examples of the types of transmissions and third-party recipients involved, illustrating how the practices described above were implemented during Plaintiff's visit to Defendant's Website.

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

83. Given the number of Internet users, the "world's most valuable resource is no longer oil, but data."[23]

84. Consumers' web browsing histories have an economic value of 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.[24]

85. There is a "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."[25]

86. Extracted personal data can be used to design products, platforms, and marketing techniques. A study by the McKinsey global consultancy concluded that businesses that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[26]

87. 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

---

[23] 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

[24] *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).

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

[26] 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

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.[27]

88. 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.[28]

89. 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.

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

91. By implementing Trackers on the Website, Defendant participates in building detailed behavioral profiles of visitors. These profiles include information such

[27] 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

[28] 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.

as which users viewed specific products, whether they initiated but abandoned the checkout process, and what pages or buttons they interacted with. This data enables Defendant and its advertising partners to identify repeat visits from the same device or browser. This 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 users who showed purchase intent, 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.

92. 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 the privacy implications to users.

93. 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).

/ / /

94. 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. Defendant's Conduct Constitutes An Invasion Of Plaintiff's And Class Members' Privacy

95. The collection of Plaintiff's and Class Members' personally identifying, de-anonymized information through Defendant's installation and use of the Trackers constitutes an invasion of privacy.

96. As alleged herein, the Trackers are designed to conduct targeted advertising and boost Defendant's revenue, all through their surreptitious collection of Plaintiff's and Class Members' personal information.

97. To put the invasiveness of Defendant's violations of the CIPA into perspective, it is also important to understand three concepts: data brokers, real-time bidding, and cookie syncing.

98. In short, the import of these concepts is that: (i) the Third Parties are data brokers (or partner with data brokers) that collect user information from Website visitors to uniquely identify and de-anonymize users by combining their IP addresses, Device Metadata, User Information, and unique user ID values with whatever information those Third Parties have on a user from other sources; (ii) the Third Parties share that information with other entities to create the most complete user profile they can (through cookie syncing), which includes a more complete and non-anonymous portrait of the user; and (iii) those profiles are offered up for sale through the real-time bidding process

to the benefit of Defendant and the Third Parties and to the detriment of users' privacy interests.

a. Data Brokers And Real-Time Bidding: The Information Economy

Data Brokers

99. While "[t]here is no single, agreed-upon definition of data brokers in United States law,"[29] California law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct [*i.e.*, consumer-facing] relationship," subject to certain exceptions. Cal. Civ. Code § 1798.99.80(c).

100. Any entity that qualifies as a "data broker" under California law must specifically register as such Cal. Civ. Code § 1798.99.82(a). Here, the ComScore tracker is operated by a registered California data broker.

101. "Data brokers typically offer pre-packaged databases of information to potential buyers," either through the "outright s[ale of] data on individuals" or by "licens[ing] and otherwise shar[ing] the data with third parties."[30] Such databases are extensive, and can "not only include information publicly available [such as] from Facebook but also the user's exact residential address, date and year of birth, and political affiliation," in addition to "inferences [that] can be made from the combined data."[31]

102. For instance, the NATO report noted that data brokers collect two sets of information: "observed and inferred (or modelled)." The former "is data that has been collected and is actual," such as websites visited." Inferred data "is gleaned from

[29] JUSTIN SHERMAN, DUKE SANFORD CYBER POLICY PROGRAM, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS: THREATS TO AMERICAN CIVIL RIGHTS, NATIONAL SECURITY, AND DEMOCRACY, at 2 (DUKE SANFORD CYBER POLICY PROGRAM, 2021), https://tinyurl.com/hy9fewhs.

[30] SHERMAN, *supra*, at 2.

[31] Tehila Minkus et al., *The City Privacy Attack: Combining Social Media and Public Records for Detailed Profiles of Adults and Children*, COSN '15: PROCEEDINGS OF THE 2015 ACM ON CONFERENCE ON ONLINE SOCIAL NETWORKS 71, 71 (2015), https://dl.acm.org/doi/pdf/10.1145/2817946.2817957.

observed data by modelling or profiling," meaning what users may be *expected* to do. On top of this, "[b]rokers typically collect not only what they immediately need or can use, but hoover up as much information as possible to compile comprehensive data sets that might have some future use."[32]

103. Likewise, a report by the Duke Sanford Cyber Policy Program "examine[d] 10 major data brokers and the highly sensitive data they hold on U.S. individuals."[33] The report found that "data brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees."[34]

104. This data collection has grave implications for Americans' right to privacy. For instance, "U.S. federal agencies from the Federal Bureau of Investigation [] to U.S. Immigration and Customs Enforcement [] purchase data from data brokers—without warrants, public disclosures, or robust oversight—to carry out everything from criminal investigations to deportations."[35]

105. As another example:

> Data brokers also hold highly sensitive data on U.S. individuals such as race, ethnicity, gender, sexual orientation, immigration status, income level, and political preferences and beliefs (like support for the NAACP or National LGBTQ Task Force) that can be used to directly undermine individuals' civil rights. Even if data brokers do not explicitly advertise these types of data (though in many cases they do), everything from media reporting to testimony by a Federal Trade Commission commissioner has identified the risk that data brokers use their data sets to make "predictions" or "inferences" about this kind of sensitive

[32] TWETMAN & BERGMANIS-KORATS, *supra*, at 11.
[33] SHERMAN, *supra*, at 1.
[34] *Id*.
[35] *Id.* at 9.

> information (race, gender, sexual orientation, etc.) on individuals.
> This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements. Many
> industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services.
> …
>
> Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups.[36]

106. Similarly, as the report from NATO noted, corporate data brokers cause numerous privacy harms, including but not limited to depriving users of the right to control who does and does not acquire their personal information, unwanted advertisements that can even go as far as manipulating viewpoints, and spam and phishing attacks.[37]

/ / /

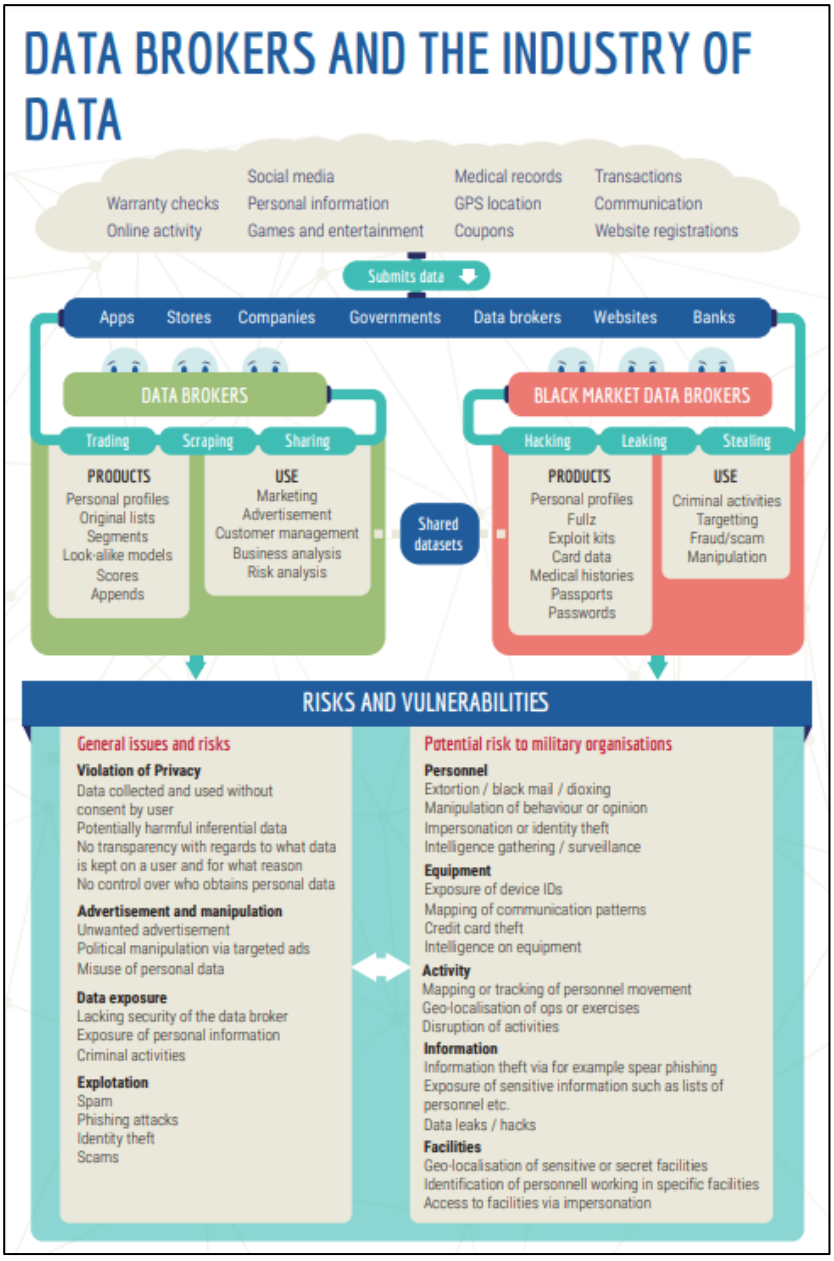
/ / /

/ / /

[36] *Id*.

[37] TWETMAN & BERGMANIS-KORATS, *supra*, at 8.

Figure 4:



107. As noted above, data brokers are able to compile such wide swaths of information in part by collecting users' IP addresses, Device Metadata, and User Information, which is used by data brokers to track users across the Internet.[38]

/ / /

[38] *Id.* at 11.

108. Indeed, as McAfee (a data security company) notes, "data brokers can … even place trackers or cookies on your browsers … [that] track your IP address and browsing history, which third parties can exploit."[39]

109. These data brokers will then:

> take that data and pair it with other data they've collected about you, pool it together with other data they've got on you, and then share all of it with businesses who want to market to you. They can eventually build large datasets about you with things like: "browsed gym shorts, vegan, living in Los Angeles, income between $65k-90k, traveler, and single." Then, they sort you into groups of other people like you, so they can sell those lists of like-people and generate their income.[40]

110. In short, by collecting IP addresses Device Metadata, and User Information, data brokers and many of the entities the Third Parties sync with can track users across the Internet, compiling various bits of information about users, building comprehensive user profiles that include an assortment of information, interests, and inferences, and offering up that information for sale to the highest bidder. The "highest bidder" is a literal term, as explained below.

111. As a result of Defendant's installation of trackers operated by data brokers like ComScore, and by numerous third parties with which those brokers synchronize, the information of Plaintiff and Class Members is linked to existing profiles maintained by those brokers, or used to generate new ones. This linkage occurs through the collection of IP addresses, device metadata, and other user information from the browsers of Defendant's Website visitors.

/ / /

[39] Jasdev Dhaliwal, *How Data Brokers Sell Your Identity*, MCAFEE (June 4, 2024), https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/.

[40] Paul Jarvis, *The Problem with Data Brokers: Targeted Ads and Your Privacy*, FATHOM ANALYTICS (May 10, 2022), https://usefathom.com/blog/data-brokers.

112. These profiles are then served up to any companies that want to advertise on Defendant's Website, and Defendant's users become more valuable as a result of having their IP addresses, Device Metadata, and User Information linked to these data broker profiles. Thus, Defendant is unjustly enriched through advertising revenue by installing the Trackers on Plaintiff's and Class Members' browsers, and thus, enabling the Third Parties to collect Plaintiff's and Class Members' IP addresses, Device Metadata, and User Information without consent.

Real-Time Bidding

113. Once data brokers and many of the entities the Third Parties sync with collect Website users' IP addresses, Device Metadata, and User Information, how do they "sell" or otherwise help Defendant monetize that information? This is where real-time bidding comes in.

114. "Real Time Bidding (RTB) is an online advertising auction that uses sensitive personal information to facilitate the process to determine which digital ad will be displayed to a user on a given website or application."[41]

115. "There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs)." An SSP work[s] with website or app publishers to help them participate in the RTB process." "DSPs primarily work with advertisers to help them "[r]each relevant audiences on the open internet, drive growth, and prove your impact.."[42] And an Advertising Exchange "allows advertisers and publishers to use the same technological platform, services, and methods, and 'speak the same language' in order to exchange data, set prices, and ultimately serve an ad."[43]

/ / /

[41] Sara Geoghegan, *What is Real Time Bidding?*, ELECTRONIC PRIVACY INFORMATION CENTER (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/.

[42] *Id.*

[43] *Introducing To Ad Serving*, MICROSOFT IGNITE (Mar. 3, 2024), https://learn.microsoft.com/en-us/xandr/industry-reference/introduction-to-ad-serving.

116. In other words, SSPs provide user information to advertisers that might be interested in those users, a DSP like DoubleClick is the platform on which all of this happens.

117. The RTB process works as follows:

> After a user loads a website or app, an SSP will send user data to Advertising Exchanges … The user data, often referred to as "bidstream data," contains information like device identifiers, IP address, zip/postal code, GPS location, browsing history, location data, and more. After receiving the bidstream data, an Advertising Exchange will broadcast the data to several DSPs [here, DoubleClick]. The DSPs will then examine the broadcasted data to determine whether to make a bid on behalf of their client.
>
> Ultimately, if the DSP wins the bid, its client's advertisement will appear to the user. Since most RTB auctions are held on the server/exchange side, instead of the client/browser side, the user only actually sees the winner of the auction and would not be aware of the DSPs who bid and lost. But even the losing DSPs still benefit because they also receive and collect the user data broadcasted during the RTB auction process. This information can be added to existing dossiers DSPs have on a user.[44]

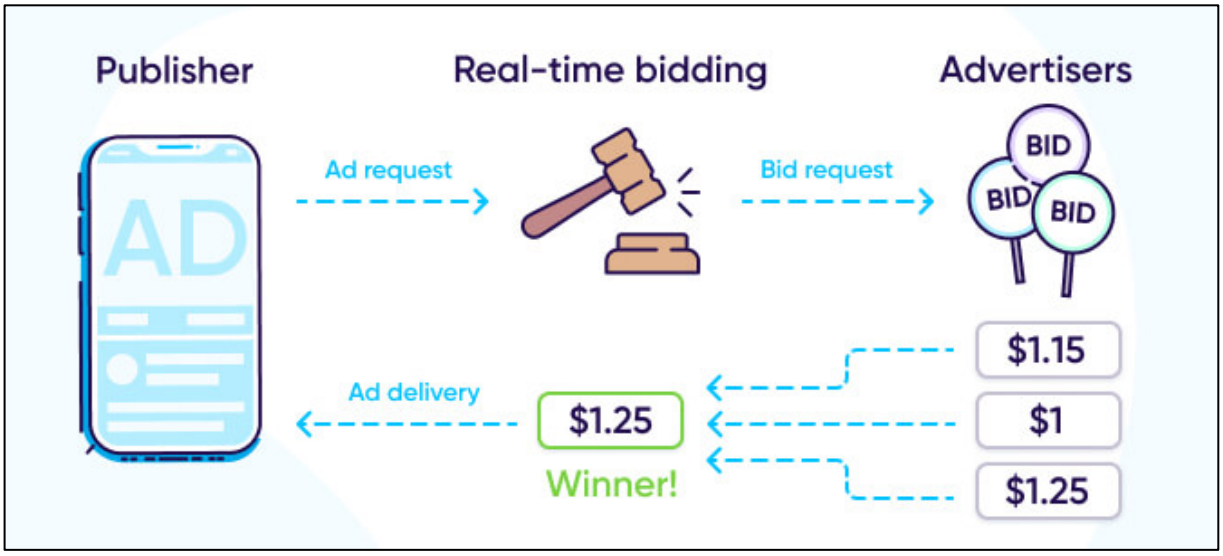
/ / /

/ / /

/ / /

[44] Geoghegan, *supra*; *see also* REAL-TIME BIDDING, APPSFLYER, https://www.appsflyer.com/glossary/real-time-bidding/.

Figure 5:



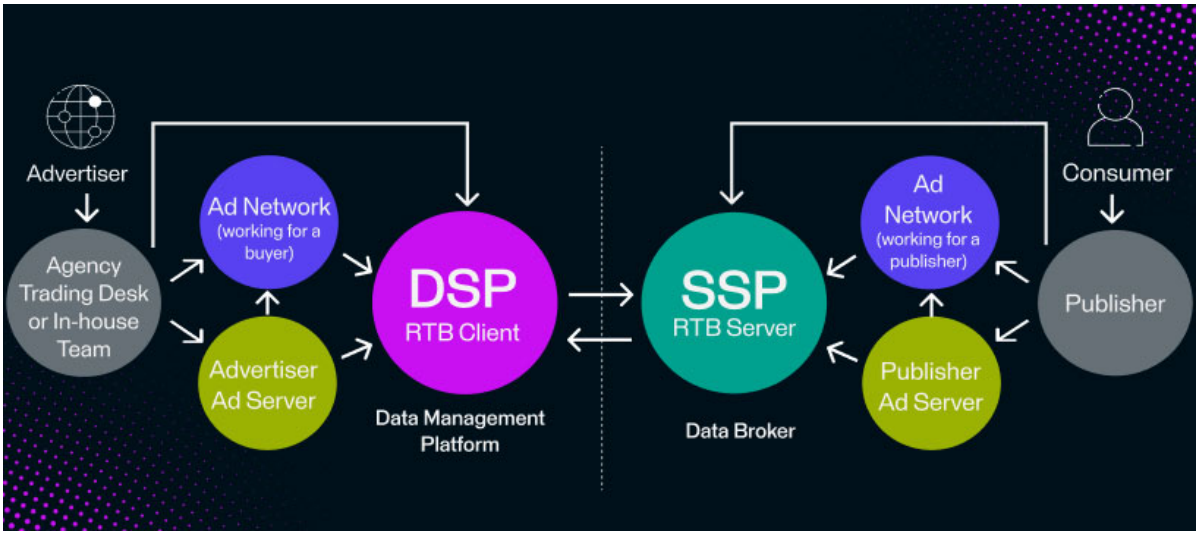
118. Facilitating this real-time bidding process means SSPs and DSPs must have as much information as possible about Defendant's users to procure the greatest interest from advertisers and the highest bids. These entities receive assistance because Defendant also installs the trackers of data brokers on its users' browsers:

> the economic incentives of an auction mean that DSP [or SSP] with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The DSP enlists a final actor, the data management platform (DMP) [or a data broker]. DSPs [or SSPs] send bid requests to DMPs [and data brokers], who enrich them by attempting to identify the user in the request and use a variety of data sources, such as those uploaded by the advertiser, collected from other sources, or bought from data brokers. The DSP with the highest bid not only wins the right to deliver the ad—through the SSP—to the individual. The DSP also wins the right to cookie sync its own cookies with those from the [Advertising Exchange], thus enabling easier linkage of the data to the user's profile in the future.[45]

/ / /

[45] Michael Veale & Federik Zuiderveen Borgesius, *Adtech and Real-Time Bidding under European Data Protection Law*, 23 GERMAN L. J. 226, 232-33 (2022) https://tinyurl.com/yjddt5ey.

Figure 6:



119. In other words, SSPs can solicit the highest bids for Website users by identifying and de-anonymizing those users by combining the information they know about that user with the information other data brokers know about that user. If there is a match, then the SSPs will have significantly more information to provide about users, and that will solicit significantly higher bids from prospective advertisers (because the advertisers will have more information about the user to target their bids).

120. Likewise, a DSP like DoubleClick can generate the highest and most targeted bids from advertisers with providing those advertisers with as much information about users as possible, which it does by syncing with data brokers who, in turn, sync with other data brokers and/or are data brokers themselves.

121. All of this naturally enriches Defendant, as its users have now become more valuable thanks to the replete information the Third Parties are able to provide about users.

122. As the Federal Trade Commission ("FTC") has noted, "[t]he use of real-time bidding presents potential concerns," including but not limited to:

/ / /

a. "incentiviz[ing] invasive data-sharing" by "push[ing] publishers [*i.e.*, Defendant] to share as much end-user data as possible to get higher valuation for their ad inventory—particularly their location data and cookie cache, which can be used to ascertain a person's browsing history and behavior."

b. "send[ing] sensitive data across geographic borders."

c. sending consumer data "to potentially dozens of bidders simultaneously, despite only one of those parties—the winning bidder actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring those other parties do not retain that data for use in unintended ways."[46]

123. Given DoubleClick operates as DSP's here, the last point is particularly relevant, as it means Google collects and discloses Website users' information to *all prospective advertisers*, even if advertisers do not ultimately show a user an advertisement. This greatly diminishes the ability of users to control their personal information.

124. Likewise, the Electronic Privacy Information Center ("EPIC") has warned that "[c]onsumers' privacy is violated when entities disclose their information without authorization or in ways that thwart their expectations."[47]

125. For these reasons, some have characterized "real-time bidding" as "[t]he biggest data breach ever recorded" because of the shear number of entities that receive personal information[48]:

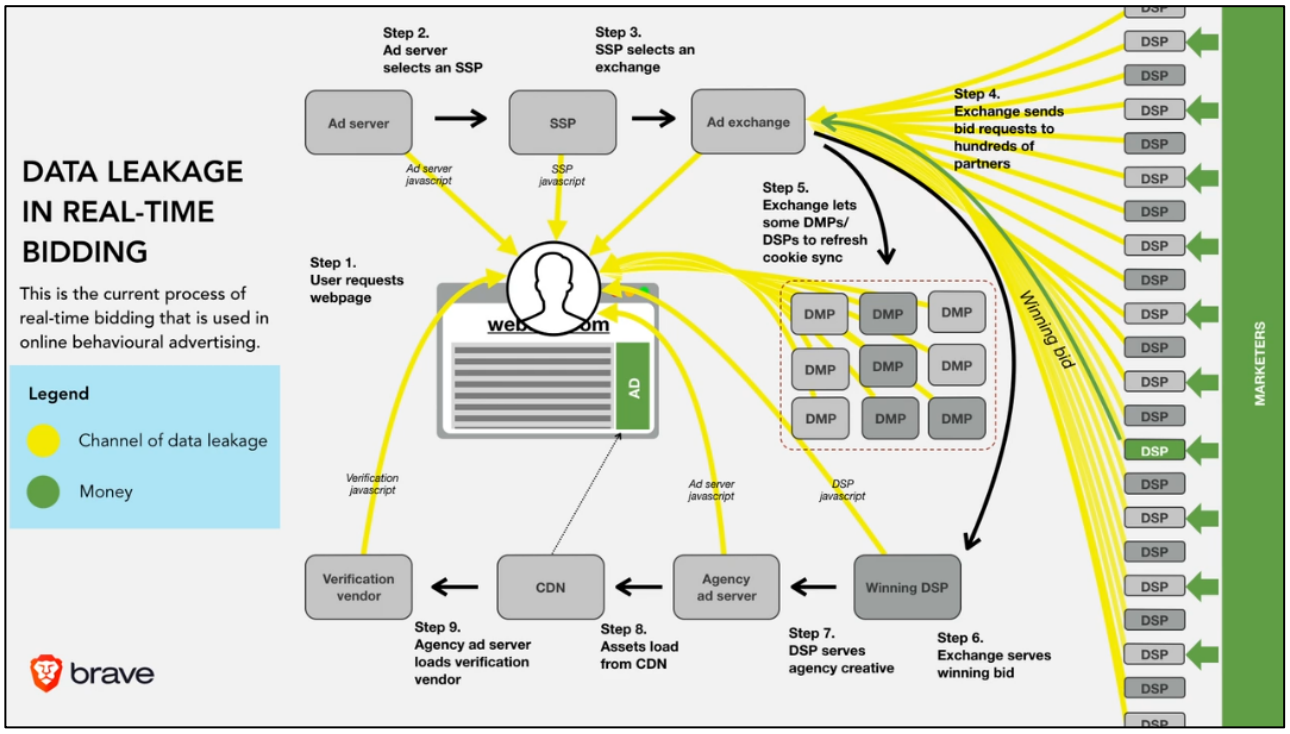
/ / /

[46] FEDERAL TRADE COMMISSION, UNPACKING REAL TIME BIDDING THROUGH FTC'S CASE ON MOBILEWALLA (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla.

[47] Geoghegan, *supra*.

[48] DR. JOHNNY RYAN, "RTB" ADTECH & GDPR, https://assortedmaterials.com/rtb-evidence/ (video).

Figure 7:



126. All of this is in line with protecting the right to determine who does and does not get to know one's information, a harm long recognized at common law and one the CIPA was enacted to protect against. *Ribas v. Clark*, 38 Cal. 3d 355 361 (1985) (noting the CIPA was drafted with a two-party consent requirement to protect "the right to control the nature and extent of the firsthand dissemination of [one's] statements"); *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press* 489 U.S. 749, 763-64 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

Cookie Syncing

127. It should now be clear both the capabilities of the Third Parties (*i.e.*, data brokers like ComScore who de-anonymize users, or companies who sync with data brokers for this purpose) and the reasons Defendant installs their Trackers on its Website (to sell to advertisers in real-time bidding with as much information about users as possible to solicit the highest bids). The final question is how do these Third Parties

share information amongst each other and with others to offer the most complete user profiles up for sale? This occurs through "cookie syncing."

128. Cookie syncing is a process that "allow[s] web companies to share (synchronize) cookies, and match the different IDs they assign for the same user while they browse the web."[49] This allows entities like the Third Parties to circumvent "the restriction that sites can't read each other cookies, in order to better facilitate targeting and real-time bidding."[50]

129. Cookie syncing ("CSync") works as follows:

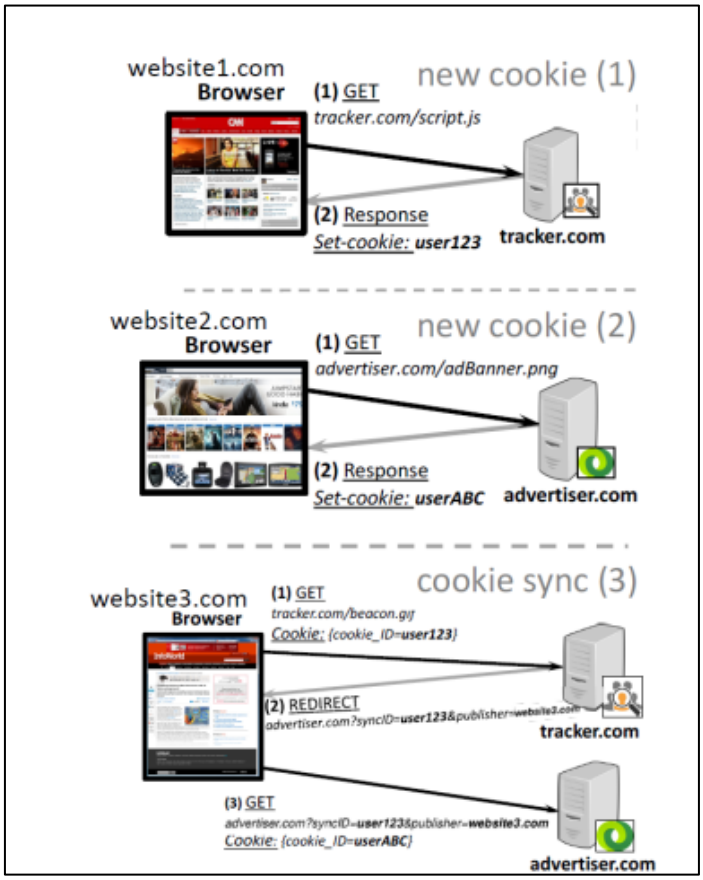
> Let us assume a user browsing several domains like website1.com and website2.com, in which there are 3rd-parties like tracker.com and advertiser.com, respectively. Consequently, these two 3rd-parties have the chance to set their own cookies on the user's browser, in order to re-identify the user in the future. Hence, tracker.com knows the user with the ID user123, and advertiser.com knows the same user with the ID userABC.
>
> Now let us assume that the user lands on a website (say website3.com), which includes some JavaScript code from tracker.com but not from advertiser.com. Thus, advertiser.com does not (and cannot) know which users visit website3.com. However, *as soon as the code of tracker.com is called, a GET request is issued by the browser to tracker.com (step 1), and it responds back with a REDIRECT request (step 2), instructing the user's browser to issue another GET request to its collaborator advertiser.com this time, using a specifically crafted URL (step 3)*.
>
> …

[49] Panagiotis Papadopoulos et al., *Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask*, 1 WWW '19: THE WORLD WIDE WEB CONFERENCE 1432, 1432 (2019), https://dl.acm.org/doi/10.1145/3308558.3313542.

[50] Gunes Acar et al., *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*, 6B CCS'14: ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 674, 674 (2014)

When advertiser.com receives the above request along with the cookie ID userABC, it finds out that userABC visited website3.com. *To make matters worse, advertiser.com also learns that the user whom tracker.com knows as user123, and the user userABC is basically one and the same user.* Effectively, CSync enabled advertiser.com to collaborate with tracker.com, in order to: (i) find out which users visit website3.com, and (ii) *synchronize (i.e., join) two different identities (cookies) of the same user on the web*.[51]

Figure 8:



130. Through this process, third party trackers are not only able to resolve user identities (*e.g.*, learning that who Third Party #1 knew as "userABC" and Third Party #2 knew as "user123" are the same person), they can "track a user to a much larger number of websites," even though that "do not have any collaboration with" the third party.[52]

[51] Papadopoulos, *supra*, at 1433.
[52] Papadopoulos, *supra*, at 1434.

131. On the flip side, "CSync may re-identify web users even after they delete their cookies."[53] "[W]hen a user erases her browser state and restarts browsing, trackers usually place and sync a new set of userIDs, and eventually reconstruct a new browsing history."[54] But if a tracker can "respawn" its cookie or like to another persistent identifier (like an IP address), "then through CSync, all of them can link the user's browsing histories from before and after her state erasure. Consequently: (i) users are not able to abolish their assigned userIDs even after carefully erasing their set cookies, and (ii) trackers are enabled to link user's history across state resets."[55]

132. Thus, "syncing userIDs of a given user increases the user identifiability while browsing, thus reducing their overall anonymity on the Web."[56]

133. The tracking activity at issue does not depend on users remaining anonymous. When the Trackers deployed on the Website execute within a user's browser, they assign and transmit persistent identifiers and related signaling data to their respective third-party operators as part of ordinary analytics, advertising, and session-measurement functions. As a result, the same browser or device can be recognized across multiple pageviews and visits to the Website by those third parties. This persistence allows third-party platforms to associate a user's browsing activity with an identifiable browser or device profile over time, thereby eliminating true anonymity during visits to the Website, even in the absence of account login or user-provided identifying information.

134. To summarize the proceeding allegations, data brokers focus on collecting as much information about Website users as possible to create comprehensive user profiles, and the Trackers sync with numerous other data brokers that do the same. The Third Parties collect IP addresses, Device Metadata, User Information, and unique user IDs in the first instance, but those pieces of information are connected to information the

[53] *Id.*
[54] *See id.*
[55] *Id.*
[56] *Id.* at 1441.

Third Parties glean from other sources (*e.g.*, various data brokers) to build comprehensive profiles. Through "cookie syncing," those profiles are shared amongst the Third Parties and with other entities to form the most fulsome picture with the most attributes as possible. And those profiles are offered up for sale to interested advertisers through real-time bidding using the Third Parties' trackers, where users will command more value the more advertisers know about a user.

135. Thus, the Third Parties enrich the value Defendant's users would otherwise command by tying the data they obtain directly from users on the Website (*e.g.*, IP addresses, Device Metadata, User Information, unique user IDs) with comprehensive user profiles.

136. Accordingly, Defendant is using the Trackers in conjunction with the Third Parties to (i) de-anonymize users, (ii) offer its users up for sale in real-time bidding, and (iii) monetize its Website by installing the Trackers and allowing the Third Parties to collect as much information about Website users as possible (without consent).

137. Thus, Defendant is unjustly enriched through their installation and use of the Trackers, which causes data to be collected by Third Parties without Plaintiff's and Class Members' consent, and that enable the Third Parties to sell Defendant's user inventory in an ad-buying system. In addition, Plaintiff and Class Members lose the ability to control their information, as their information ends up in the hands of data brokers, advertising inventory sellers, and a virtually unlimited number advertisers themselves without knowledge or consent.

138. 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.

139. 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.

140. Defendant deploys the Trackers to build a behavioral profiling and targeted advertising system. Several of these trackers are dynamically injected into the Website through tag management systems, initiating the collection of user behavior such as pageviews, navigation patterns, and session metadata. Others are directly embedded into the Website's code, firing automatically upon page load. Together, these technologies associate user behavior with device identifiers, cookies, and pseudonymous advertising IDs, facilitating the construction of persistent user profiles for advertising and marketing purposes.

141. The Trackers participate in programmatic advertising ecosystems by capturing behavioral signals from the Website and linking them to advertising audiences. These trackers enable personalized ad delivery based on users' site interactions and associate browsing activity with broader ad networks through identifier syncing. Each of these platforms sets or reads cookies to maintain persistent tracking across sessions and domains, effectively participating in workflows designed to reidentify users and expand behavioral audience segments for targeted advertising.

142. On information and belief, Google LLC, through its DoubleClick advertising technology, operates as a DSP in connection with the Website, facilitating the delivery, measurement, and optimization of advertising campaigns across third-party websites. As deployed on Defendant's Website, the DoubleClick Tracker receives DRAS information generated during users' visits, including page URLs, referrer headers, timestamps, and Google-assigned browser or device identifiers transmitted automatically during page load and navigation events. On information and belief, this

information is used by DoubleClick to recognize and classify user browsers or devices across multiple pageviews or sessions and to associate those interactions with advertising audiences and campaign identifiers for purposes of targeted advertising delivery and measurement. Through this process, navigation signals originating on the Website are incorporated into Google's advertising systems in a manner consistent with demand-side advertising operations.

V. SPECIFIC ALLEGATIONS

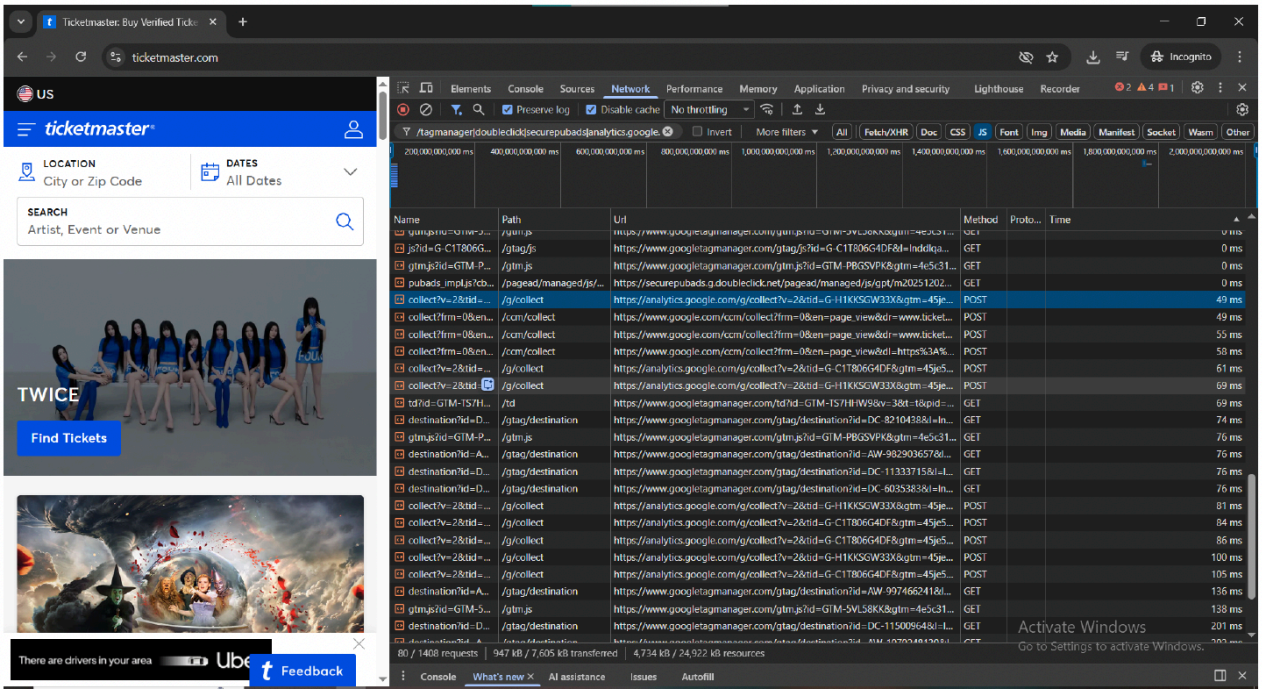
*1. The Google Tracker*s

143. Defendant embedded Google tracking technologies on the Website, including Google Tag Manager, Google Analytics (GA4), and Google Ads / DoubleClick (collectively, the "Google Trackers"). These technologies execute automatically when a user loads the Ticketmaster homepage and cause the user's browser to transmit dialing, routing, addressing, and signaling information to Google-controlled servers without any user interaction. The information transmitted includes page URLs, referrer paths, timestamps, browser and device characteristics, and Google-assigned identifiers generated as part of Google's analytics and advertising infrastructure.

144. Figure 9 is a Chrome DevTools Network capture showing a dense cluster of Google requests firing immediately upon loading Ticketmaster's homepage. The capture includes GA4 event beacons (collect?v=2), execution of Google Tag Manager and gtag.js, calls to Google Analytics collection endpoints, and advertising-related requests to securepubads.g.doubleclick.net. All of these requests occur within the initial milliseconds of page load, before any user interaction and without any consent interface visible. This figure demonstrates that Google's analytics and advertising stack is invoked automatically by the Website and begins transmitting page-level signaling information as part of the initial rendering process.

/ / /

Figure 9:



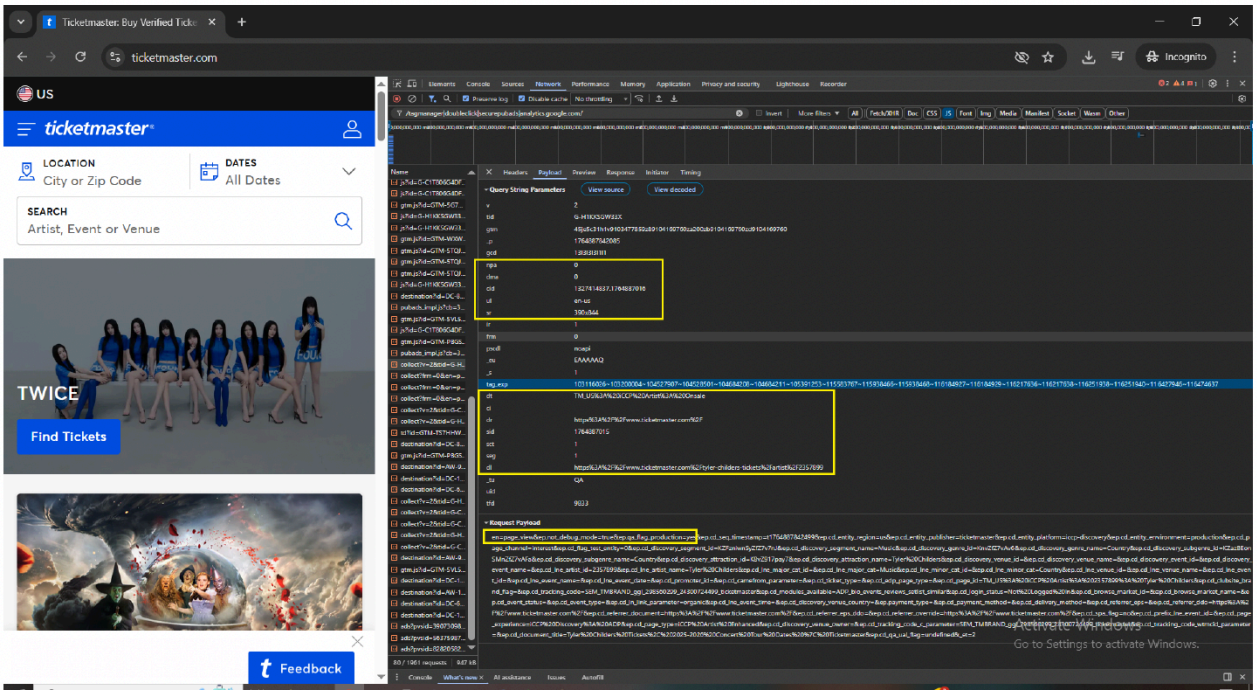
145. Figure 10 is a Chrome DevTools payload capture revealing the contents of a Google Analytics collection request generated at page load. The payload includes the full Ticketmaster page URL, referrer information, timestamped event metadata, screen resolution, Google property identifiers, and additional structured fields used for session continuity and engagement measurement. These values are transmitted at the moment the page loads and are not necessary to display content to the user. The payload demonstrates that Google receives detailed contextual, temporal, and device-level signaling information associated with the visit as part of the Website's ordinary operation.

/ / /

/ / /

/ / /

Figure 10:



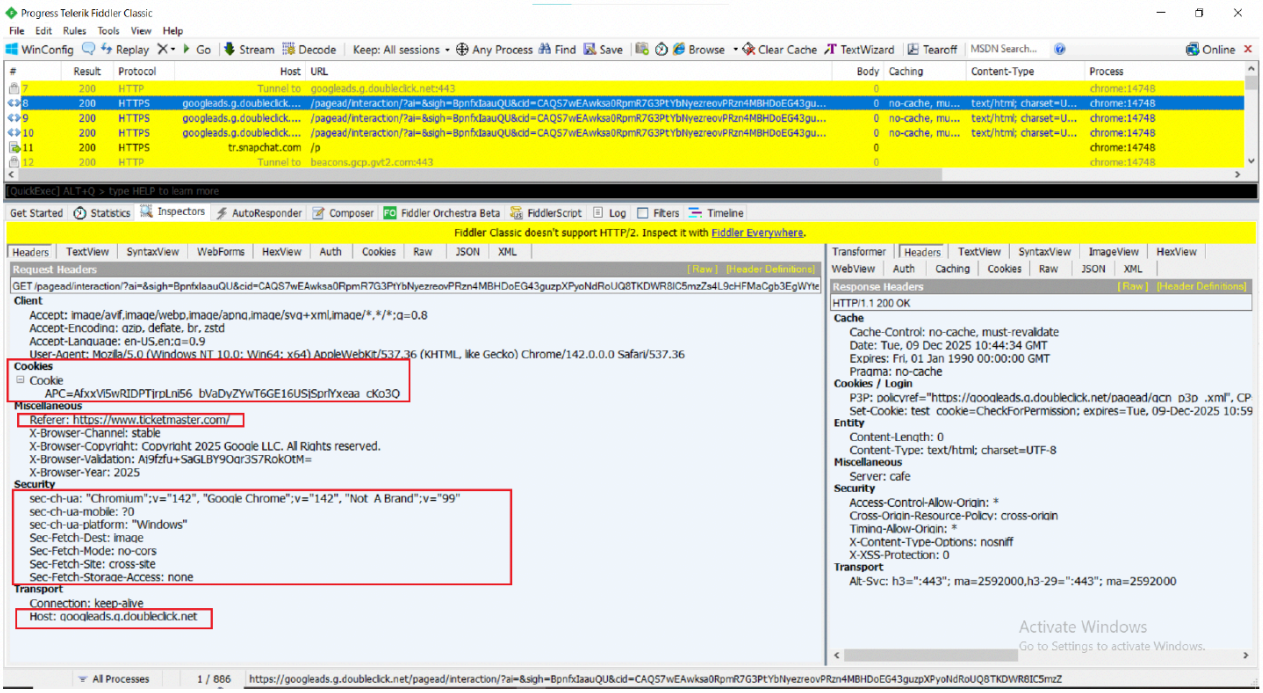
146. Figure 11 is a Fiddler capture showing the live outbound transmission of Google Ads / DoubleClick requests from the user's browser to Google advertising infrastructure. The capture reveals the transmission of Google advertising cookies, browser and device metadata contained in request headers, referrer information identifying the Ticketmaster page, and advertising-related request parameters sent to DoubleClick endpoints. This figure confirms that the signaling information observed in the browser is actually transmitted across the network to Google and that Google's advertising systems operate in parallel with Google Analytics during the same page-load sequence.

/ / /

/ / /

/ / /

Figure 11:



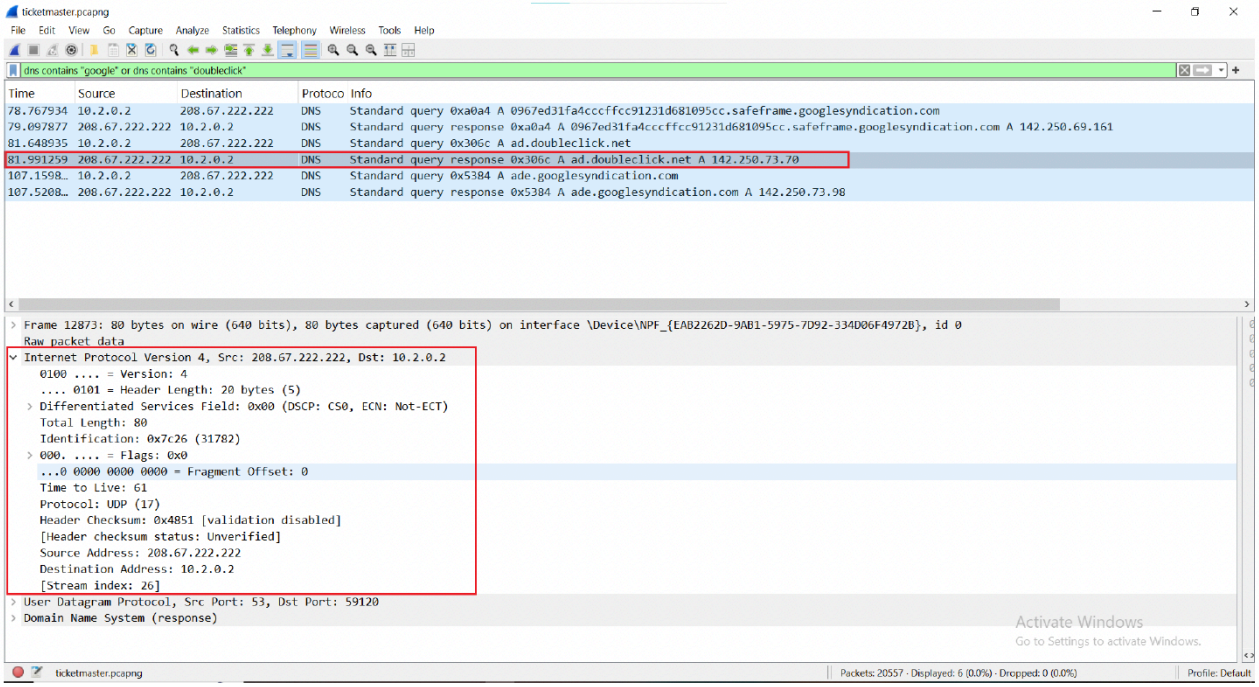
147. Figure 12 is a Wireshark capture showing DNS resolution and network routing associated with Google domains contacted during the session, including analytics and advertising endpoints. The capture identifies the client device initiating DNS queries and the resolution of those queries to Google-controlled IP addresses. This network-layer evidence corroborates that the Website-initiated Google requests observed in the browser and application layers are routed off the user's device to Google infrastructure during the initial page load.

/ / /

/ / /

/ / /

Figure 12:



148. Figures 9 through 12 together document the complete technical operation of the Google Trackers across the browser, application, and network layers. Figure 9 captures the initiation layer, showing that Google Tag Manager and related analytics and advertising code execute automatically at page load and identify the page context and referrer source. Figure 10 captures the signaling layer, showing that detailed page, device, and session metadata is packaged into Google Analytics payloads generated at load time. Figure 11 captures the transmission layer, confirming that the same visit generates live outbound requests to Google Ads / DoubleClick infrastructure carrying identifiers and routing metadata. Figure 12 captures the routing layer, independently corroborating that the user's device resolves Google domains and routes encrypted traffic to Google-controlled IP addresses during the same sequence. Taken together, these figures establish an end-to-end chain—from code execution, to data generation, to off-device transmission, to network routing—demonstrating that the Google Trackers operate as a coordinated process that captures and transmits non-content dialing, routing, addressing, and signaling information during ordinary use of the Website.

149. As shown by the foregoing, the Google Trackers constitute at least a *process* within the meaning of California Penal Code § 638.51 because they are software mechanisms that automatically execute within the user's browser and capture and transmit dialing, routing, addressing, and signaling information to Google-controlled servers. The Google Trackers also constitute at least a *device* because their operation depends on execution within the user's computing hardware, including the browser, operating system, and network interface, to generate and transmit signaling information associated with the user's visit.

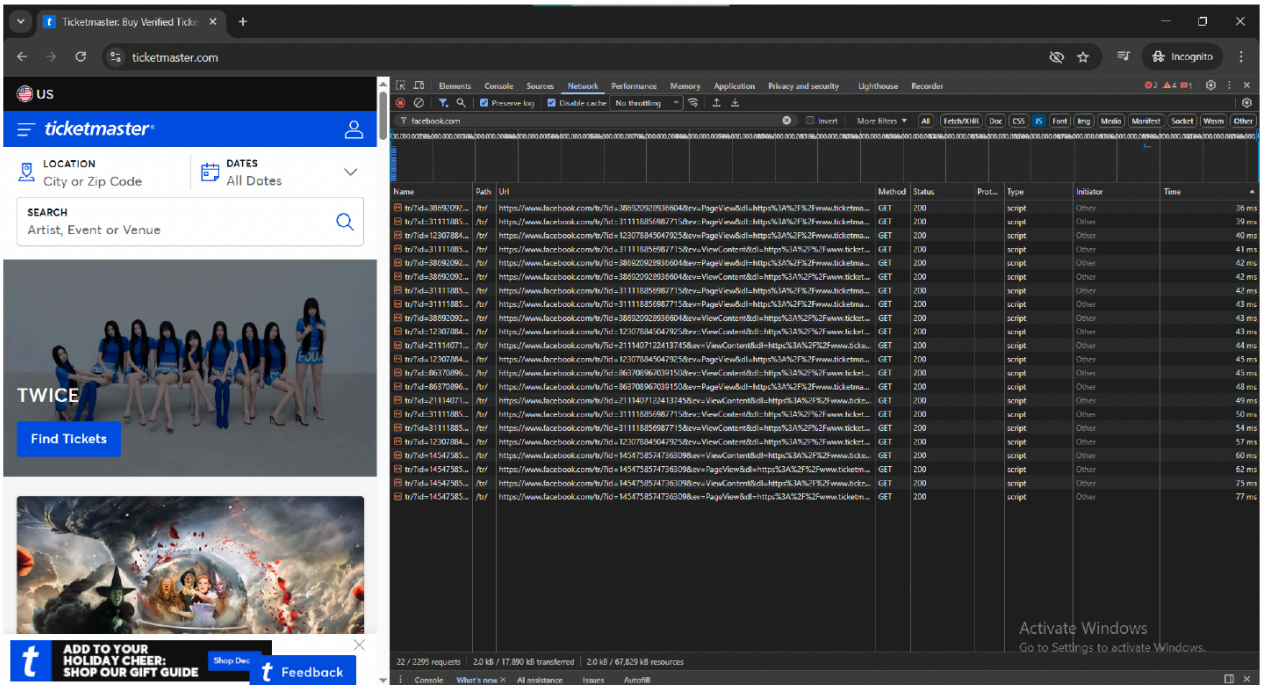
150. Defendant did not obtain a court order authorizing the installation or use of a pen register or trap-and-trace device or process and did not obtain Plaintiff's or the Class Members' consent for the deployment of the Google Trackers or for the capture and transmission of dialing, routing, addressing, and signaling information to Google.

2. The Facebook Tracker

151. Defendant embedded the Facebook tracking technology known as the Meta Pixel (the "Facebook Tracker") on the Website. The Facebook Tracker executes automatically when a user loads Ticketmaster's pages and causes the user's browser to transmit dialing, routing, addressing, and signaling information to Meta-controlled servers without any user interaction. The information transmitted includes page URLs, referrer paths, timestamps, browser and device characteristics, and Meta-assigned identifiers generated as part of Meta's advertising and measurement infrastructure.

152. Figure 13 is a Chrome DevTools Network capture showing Ticketmaster triggering multiple Facebook Pixel requests immediately upon page load, including requests associated with PageView and ViewContent events. The capture reflects requests sent to https://www.facebook.com/tr/ containing event parameters and page-specific URLs, with timestamps occurring within milliseconds of page load and prior to any user interaction. This figure demonstrates that Meta Pixel code loads automatically and transmits navigation and content-exposure signals as part of the Website's initial rendering process.

Figure 13:



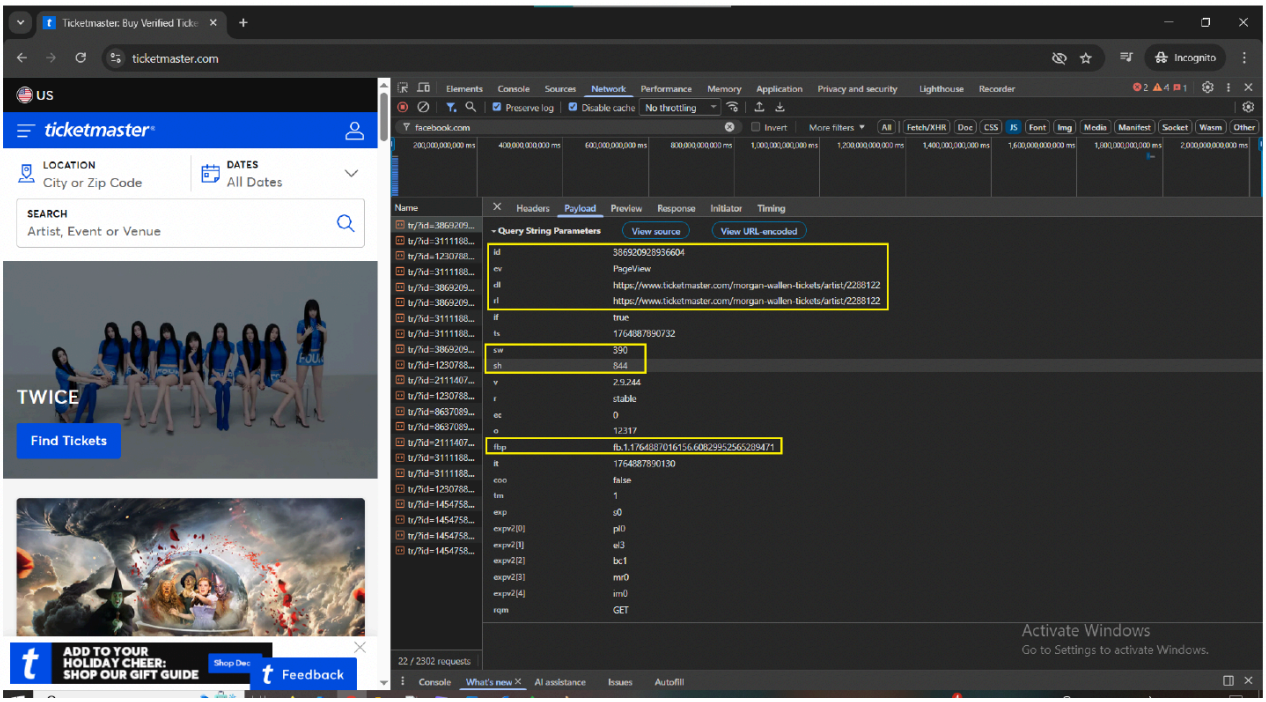
153. Figure 14 is a Chrome DevTools payload capture revealing the parameters transmitted in a Facebook Pixel request generated during page load. The payload includes the Meta Pixel ID, event type, full Ticketmaster URL, screen dimensions, timestamp values, and the _fbp browser identifier assigned by Meta. These values collectively identify the user's device environment and the specific content accessed on the Website and are transmitted automatically without any action by the user.

/ / /

/ / /

/ / /

Figure 14:



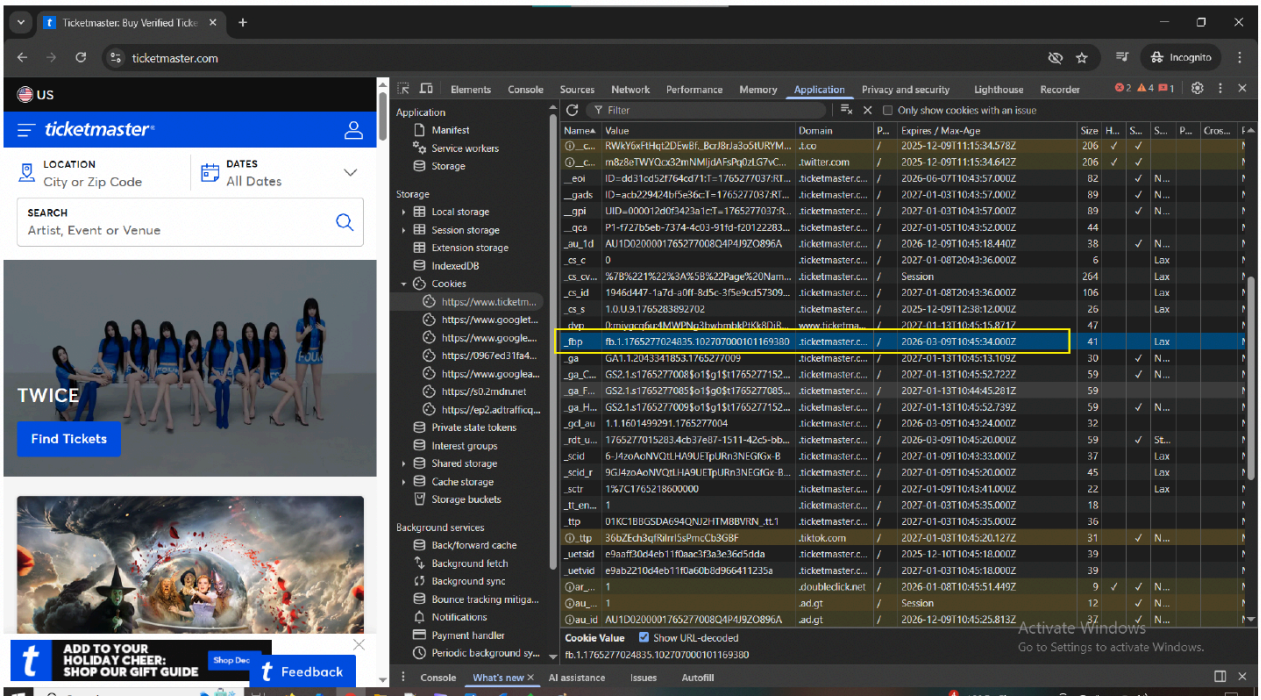
154. Figure 15 is a Chrome DevTools Application capture showing the _fbp cookie present in the user's browser prior to any consent. The cookie is stored under Ticketmaster's domain, contains a Meta-generated persistent browser identifier, and is assigned a multi-month expiration period. This figure demonstrates that Meta assigns and maintains a persistent identifier associated with the user's browser during ordinary use of the Website, enabling continuity of identification across sessions.

/ / /

/ / /

/ / /

Figure 15:



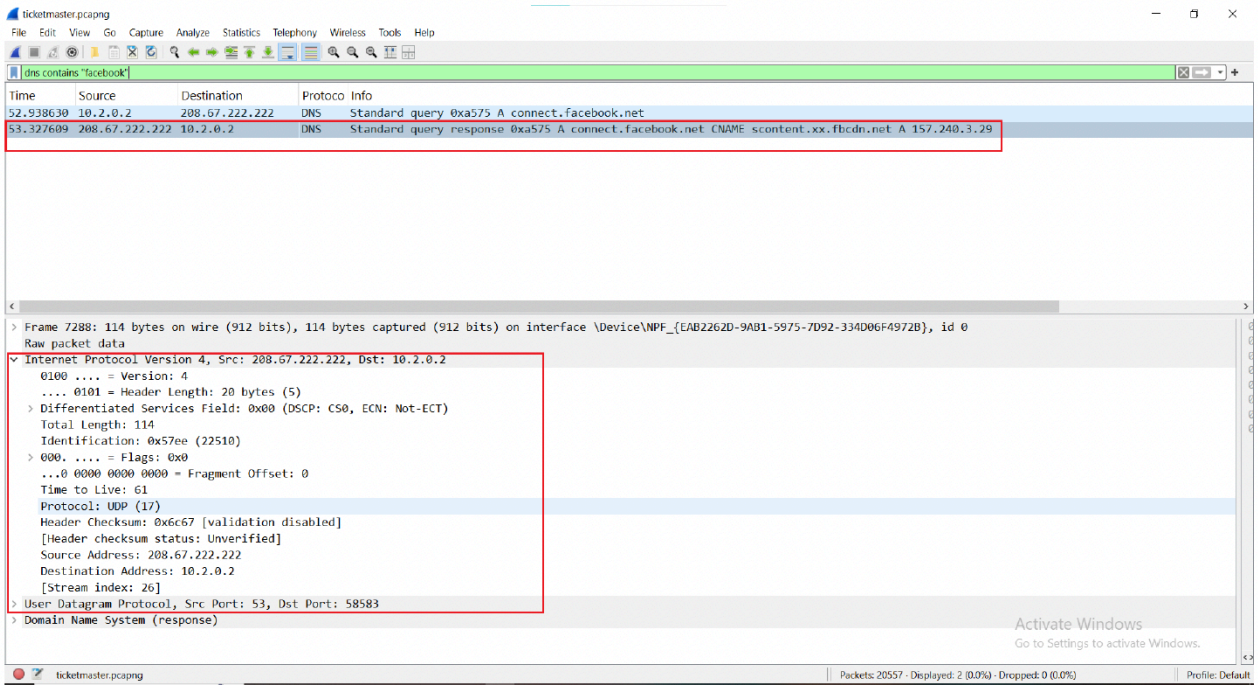
155. Figure 16 is a Wireshark capture showing DNS resolution and network routing associated with Meta domains contacted during the session, including connect.facebook.net. The capture identifies the client device initiating DNS queries and the resolution of those queries to Meta-controlled IP addresses. This network-layer evidence corroborates that the Website-initiated Facebook Pixel requests observed in the browser are routed off the user's device to Meta infrastructure during the initial page-load sequence.

/ / /

/ / /

/ / /

Figure 16:



156. Figures 13 through 16 together document the complete technical operation of the Facebook Tracker across the browser, application, and network layers. Figure 13 captures the initiation layer, showing that Meta Pixel code executes automatically at page load and transmits page-specific event data without user interaction. Figure 14 captures the signaling layer, showing that detailed page context, device attributes, timestamps, and Meta-assigned identifiers are packaged into Pixel payloads generated during the visit. Figure 15 captures the identification layer, showing the creation and presence of a persistent Meta browser identifier associated with the visit. Figure 16 captures the routing layer, independently corroborating that the user's device resolves Meta domains and routes traffic to Meta-controlled IP addresses during the same sequence. Taken together, these figures establish an end-to-end chain—from code execution, to data generation, to off-device transmission, to network routing—demonstrating that the Facebook Tracker operates as a coordinated process that captures and transmits non-content dialing, routing, addressing, and signaling information during ordinary use of the Website.

157. As shown by the foregoing, the Facebook Tracker constitutes at least a

process within the meaning of California Penal Code § 638.51 because it is a software mechanism that automatically captures and transmits dialing, routing, addressing, and signaling information to a third party. It also constitutes at least a *device* because its operation depends on execution within the user's browser and computing hardware.

158. Defendant did not obtain a court order authorizing the installation or use of a pen register or trap-and-trace device or process and did not obtain Plaintiff's or the Class Members' consent for the deployment of the Facebook Tracker or for the capture and transmission of dialing, routing, addressing, and signaling information to Meta.

3. The TikTok Tracker

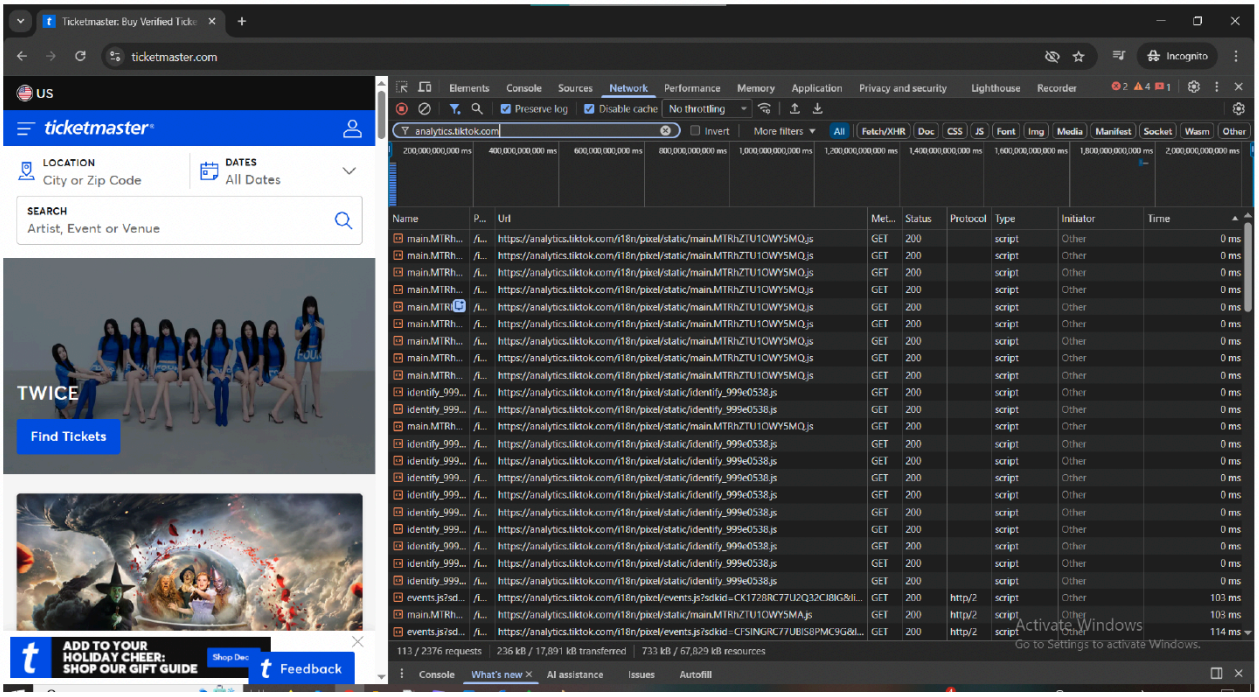
159. Defendant embedded TikTok tracking technologies, including the TikTok Pixel and associated analytics scripts (the "TikTok Tracker"), on the Website. The TikTok Tracker executes automatically when a user loads Ticketmaster's pages and causes the user's browser to transmit dialing, routing, addressing, and signaling information to TikTok-controlled servers without any user interaction. The information transmitted includes page URLs, referrer paths, timestamps, browser and device characteristics, and TikTok-assigned identifiers generated as part of TikTok's analytics and advertising infrastructure.

160. Figure 17 is a Chrome DevTools Network capture showing TikTok analytics scripts and pixel endpoints loading automatically upon page load, including requests to analytics.tiktok.com/i18n/pixel/static/, analytics.tiktok.com/pixel/events.js, and related identity and analytics modules. The timestamps reflect execution within the first milliseconds of page load, before any user interaction. This figure demonstrates that TikTok's tracking code is invoked automatically as part of the Website's initial rendering and begins generating and transmitting signaling information immediately.

/ / /

/ / /

Figure 17:



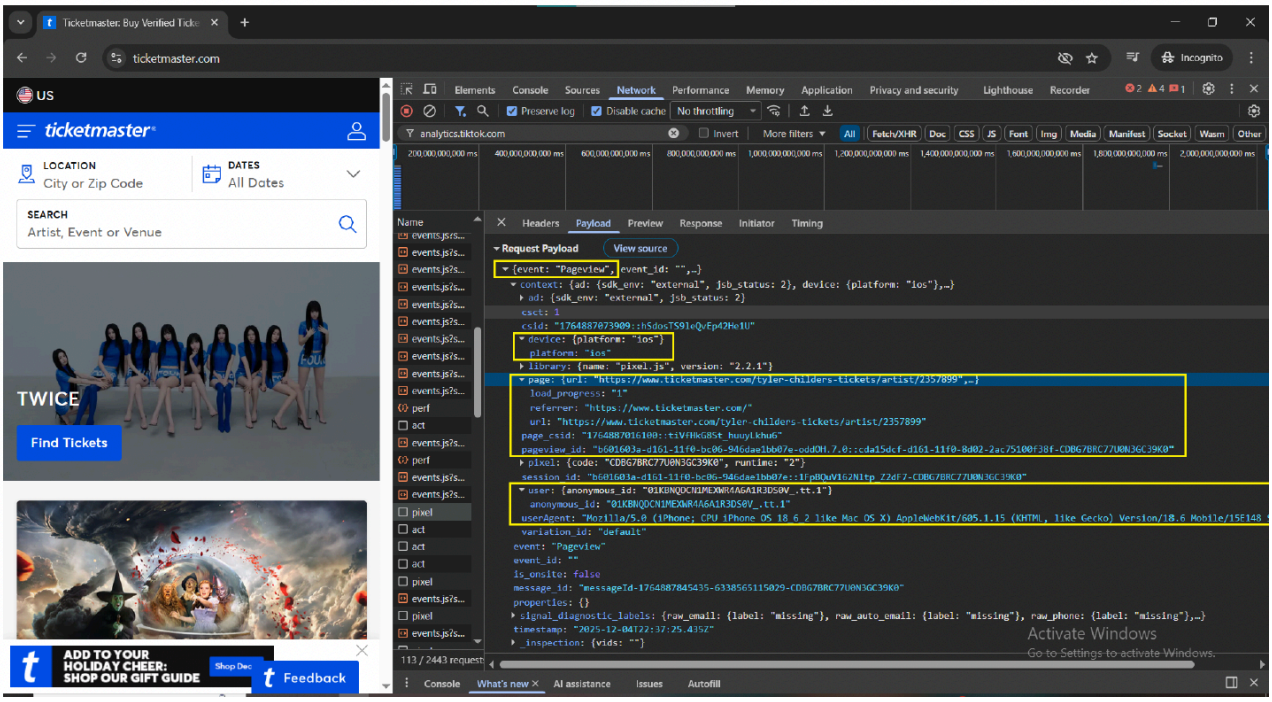
161. Figure 18 is a Chrome DevTools payload capture showing the contents of a TikTok Pixel Pageview event transmitted during page load. The JSON payload includes the event type, TikTok-generated session and event identifiers, full Ticketmaster page URL and referrer, timestamped engagement fields, platform information, and a complete user-agent string identifying the device and operating environment. These values collectively identify the user's device and precisely describe the content accessed on the Website and are transmitted automatically without any affirmative action by the user.

/ / /

/ / /

/ / /

Figure 18:



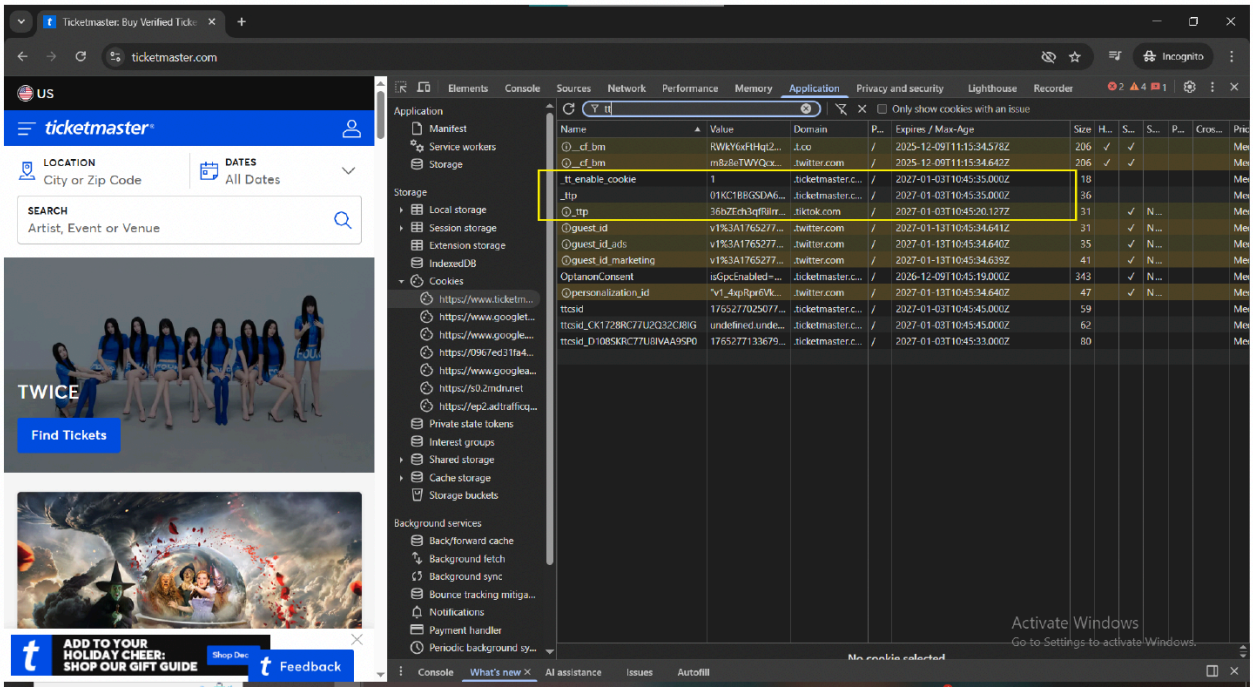
162. Figure 19 is a Chrome DevTools Application capture showing TikTok identifiers present in the user's browser prior to any consent. The capture reflects the presence of the _ttp cookie, TikTok's persistent browser identifier, and related configuration values stored with extended expiration periods. This figure demonstrates that TikTok assigns and maintains a persistent identifier associated with the user's browser during ordinary use of the Website, enabling continuity of identification across sessions.

/ / /

/ / /

/ / /

Figure 19:



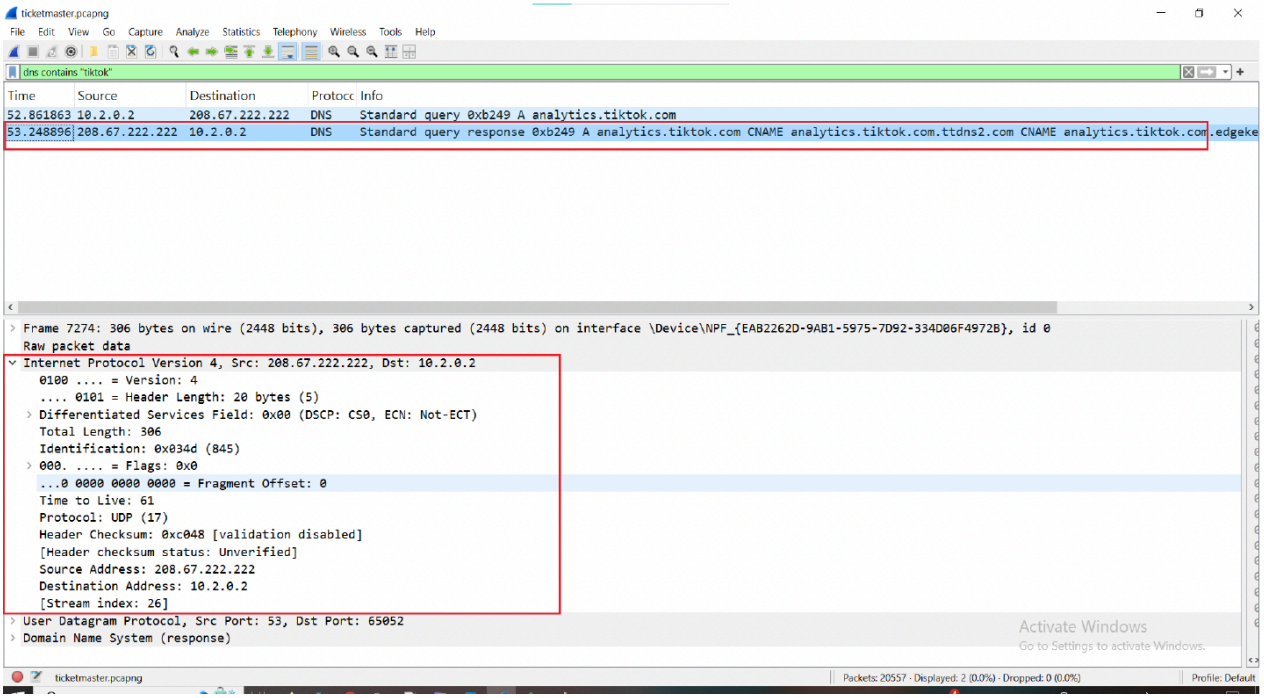
163. Figure 20 is a Wireshark capture showing DNS resolution and network routing associated with TikTok domains contacted during the session, including analytics.tiktok.com. The capture identifies the client device initiating DNS queries and the resolution of those queries to TikTok-controlled infrastructure. This network-layer evidence corroborates that the Website-initiated TikTok requests observed in the browser are routed off the user's device to TikTok servers during the initial page-load sequence.

/ / /

/ / /

/ / /

Figure 20:



164. Figures 17 through 20 together document the complete technical operation of the TikTok Tracker across the browser, application, and network layers. Figure 17 captures the initiation layer, showing that TikTok analytics and pixel code execute automatically at page load. Figure 18 captures the signaling layer, showing that detailed page context, timestamps, device attributes, and TikTok-generated identifiers are packaged into event payloads generated during the visit. Figure 19 captures the identification layer, showing the presence of a persistent TikTok browser identifier associated with the visit. Figure 20 captures the routing layer, independently corroborating that the user's device resolves TikTok domains and routes traffic to TikTok-controlled IP addresses during the same sequence. Taken together, these figures establish an end-to-end chain—from code execution, to data generation, to off-device transmission, to network routing—demonstrating that the TikTok Tracker operates as a coordinated process that captures and transmits non-content dialing, routing, addressing, and signaling information during ordinary use of the Website.

165. As shown by the foregoing, the TikTok Tracker constitutes at least a

process within the meaning of California Penal Code § 638.51 because it is a software mechanism that automatically captures and transmits dialing, routing, addressing, and signaling information to a third party. It also constitutes at least a *device* because its operation depends on execution within the user's browser and computing hardware.

166. Defendant did not obtain a court order authorizing the installation or use of a pen register or trap-and-trace device or process and did not obtain Plaintiff's or the Class Members' consent for the deployment of the TikTok Tracker or for the capture and transmission of dialing, routing, addressing, and signaling information to TikTok.

4. The Microsoft Bing Ads Tracker

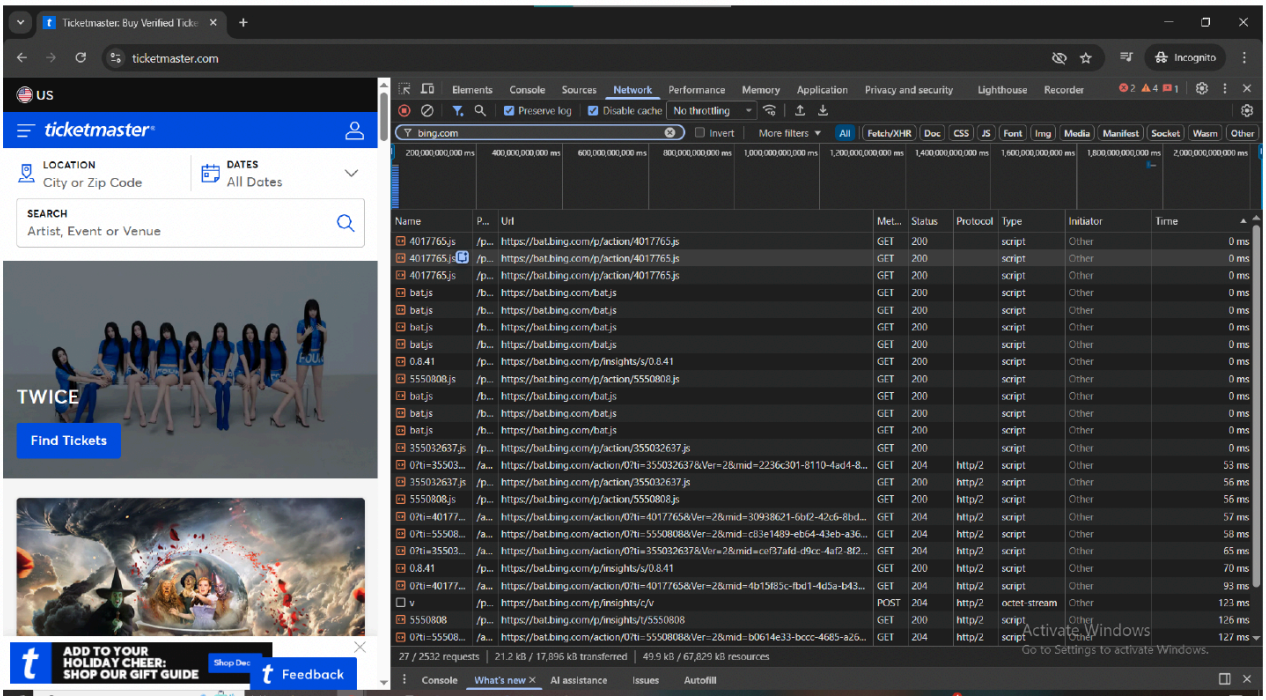
167. Defendant embedded Microsoft Bing advertising and analytics technologies, including Microsoft's Universal Event Tracking ("UET") system (the "Bing Tracker"), on the Website. The Bing Tracker executes automatically when a user loads Ticketmaster's pages and causes the user's browser to transmit dialing, routing, addressing, and signaling information to Microsoft-controlled servers without any user interaction. The information transmitted includes page URLs, referrer paths, timestamps, browser and device characteristics, and Microsoft-assigned identifiers generated as part of Microsoft's advertising and measurement infrastructure.

168. Figure 21 is a Chrome DevTools Network capture showing Microsoft Bing tracking requests loading automatically upon page load, including requests to bat.bing.com/bat.js, bat.bing.com/action, and bat.bing.com/insights. The timestamps reflect execution within the first milliseconds of page load, before any user interaction. This figure demonstrates that Microsoft's UET tracking engine is invoked automatically as part of the Website's initial rendering and begins generating and transmitting signaling information immediately.

/ / /

/ / /

Figure 21:



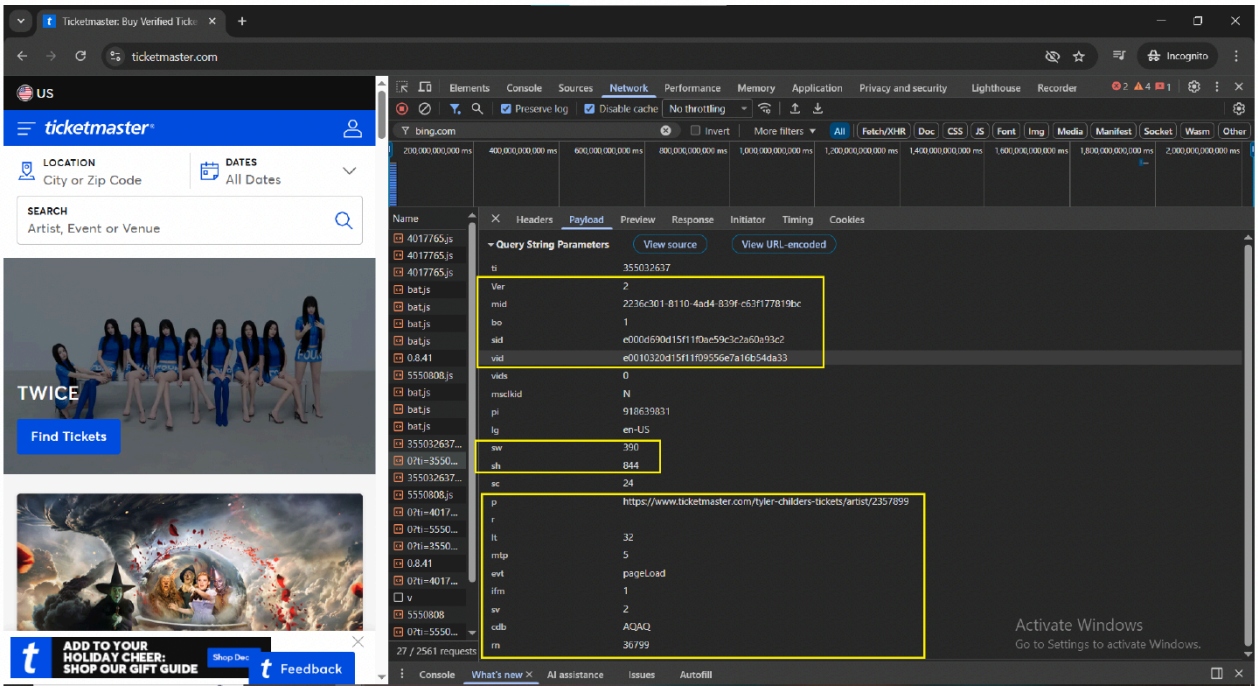
169. Figure 22 is a Chrome DevTools payload capture showing the contents of a Microsoft UET event transmitted during page load. The payload includes Microsoft-assigned identifiers such as mid, vid, and sid, screen dimensions, locale information, full Ticketmaster page URL, event metadata, and timestamped values. These parameters collectively identify the user's device environment and the specific page accessed on the Website and are transmitted automatically without any affirmative action by the user.

/ / /

/ / /

/ / /

Figure 22:



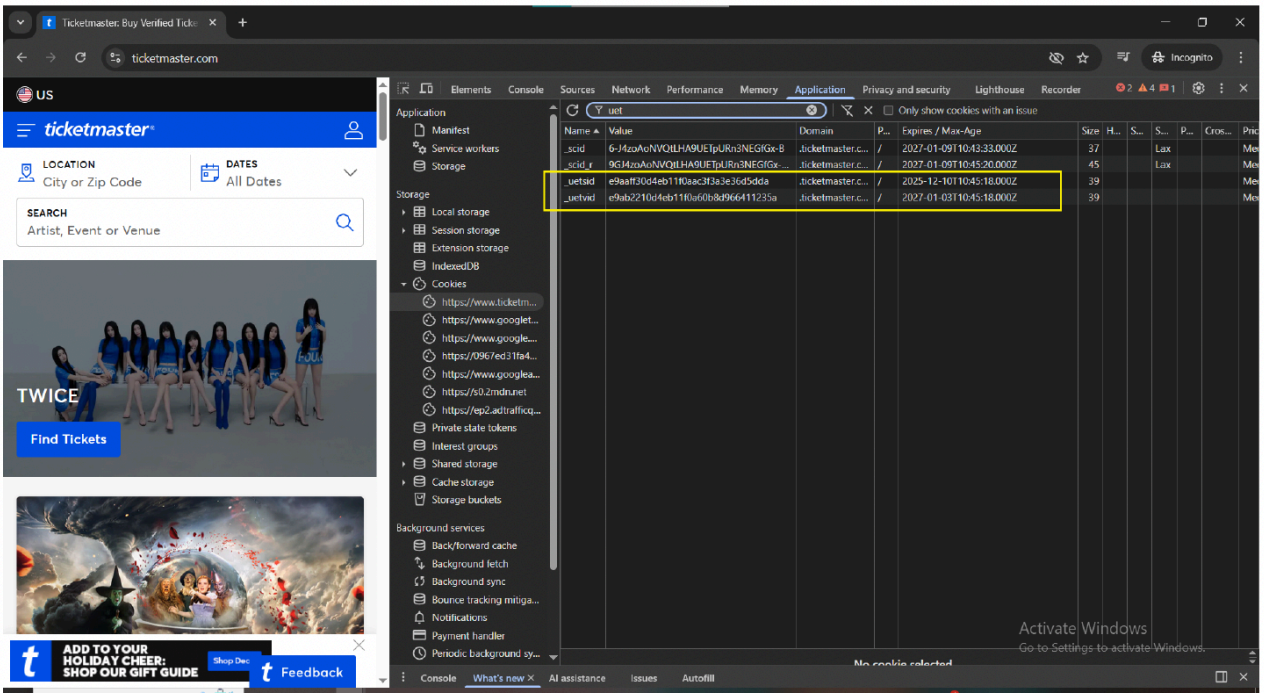
170. Figure 23 is a Chrome DevTools Application capture showing Microsoft UET cookies present in the user's browser prior to any consent, including _uetvid and _uetsid. These cookies contain persistent and session-level identifiers assigned by Microsoft and are configured with extended expiration periods. This figure demonstrates that Microsoft assigns and maintains identifiers associated with the user's browser during ordinary use of the Website, enabling recognition across sessions.

/ / /

/ / /

/ / /

Figure 23:



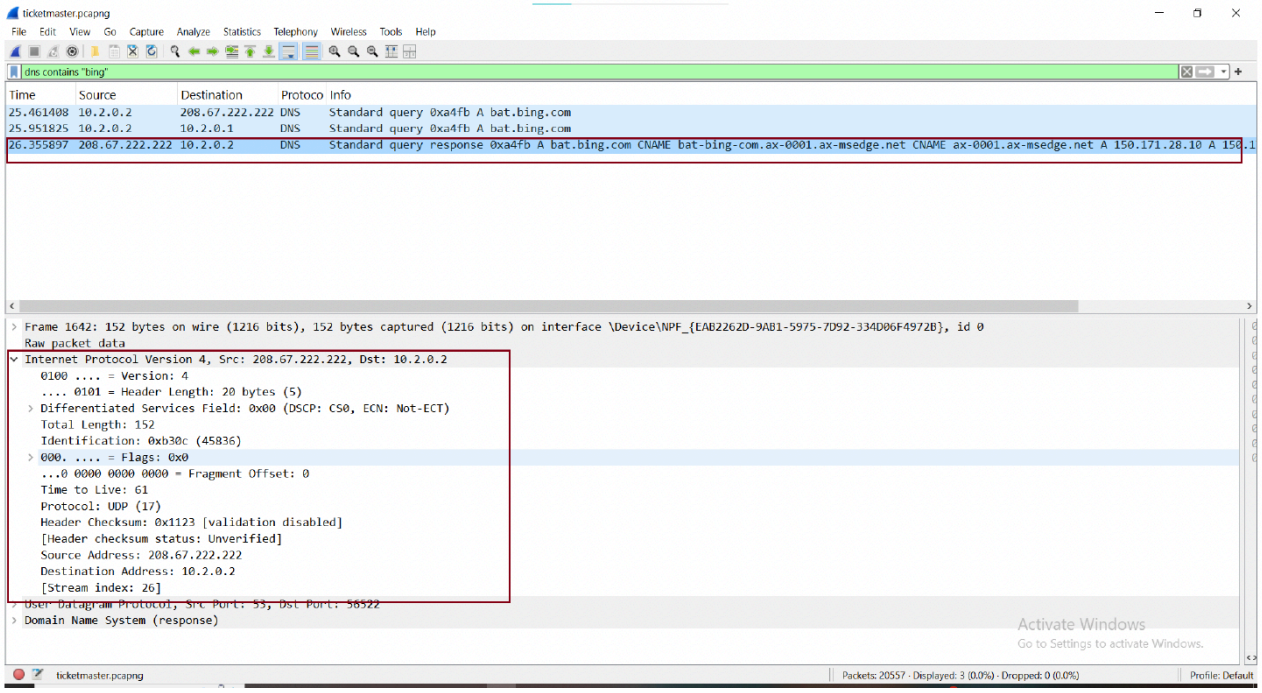
171. Figure 24 is a Wireshark capture showing DNS resolution and network routing associated with Microsoft Bing tracking domains contacted during the session, including bat.bing.com. The capture identifies the client device initiating DNS queries and the resolution of those queries to Microsoft-controlled infrastructure. This network-layer evidence corroborates that the Website-initiated Bing tracking requests observed in the browser are routed off the user's device to Microsoft servers during the initial page-load sequence.

/ / /

/ / /

/ / /

Figure 24:



172. Figures 21 through 24 together document the complete technical operation of the Bing Tracker across the browser, application, and network layers. Figure 21 captures the initiation layer, showing that Microsoft's UET scripts execute automatically at page load. Figure 22 captures the signaling layer, showing that detailed page context, timestamps, device attributes, and Microsoft-assigned identifiers are packaged into UET event payloads generated during the visit. Figure 23 captures the identification layer, showing the presence of persistent and session-level Microsoft identifiers associated with the visit. Figure 24 captures the routing layer, independently corroborating that the user's device resolves Microsoft tracking domains and routes traffic to Microsoft-controlled IP addresses during the same sequence. Taken together, these figures establish an end-to-end chain—from code execution, to data generation, to off-device transmission, to network routing—demonstrating that the Bing Tracker operates as a coordinated process that captures and transmits non-content dialing, routing, addressing, and signaling information during ordinary use of the Website.

173. As shown by the foregoing, the Bing Tracker constitutes at least a *process*

within the meaning of California Penal Code § 638.51 because it is a software mechanism that automatically captures and transmits dialing, routing, addressing, and signaling information to a third party. It also constitutes at least a *device* because its operation depends on execution within the user's browser and computing hardware.

174. Defendant did not obtain a court order authorizing the installation or use of a pen register or trap-and-trace device or process and did not obtain Plaintiff's or the Class Members' consent for the deployment of the Bing Tracker or for the capture and transmission of dialing, routing, addressing, and signaling information to Microsoft.

VI. CLASS ALLEGATIONS

175. 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.

176. **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.

177. **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 Defendant violated CIPA;
- Whether Plaintiff and Class Members are entitled to statutory damages;
- 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 the California Constitution;
- Whether the Defendant's conduct constitutes an intrusion upon seclusion;
- Whether the Defendant's conduct constitutes an unlawful, misleading, deceptive or fraudulent business practice; and
- Whether Plaintiff and the Class Members are entitled to equitable relief for unjust enrichment.

178. **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.

179. **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.

180. **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. Individualized litigation also presents a potential for inconsistent or contradictory judgments.

/ / /

/ / /

VII. FIRST CAUSE OF ACTION

Violations of Cal. Penal Code § 638.51

By Plaintiff and the Class Members Against All Defendants

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

182. Plaintiff brings this cause of action individually and on behalf of the members of the proposed Class against Defendant.

183. 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.

184. The Trackers recorded Plaintiff's dialing, routing, addressing, and signaling information in real time, automatically transmitting this dialing, routing, addressing and signaling data to multiple third-party ad-tech endpoints before the Webpage fully loaded.

185. 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 Cal. Constitution Article I § 1

By Plaintiff and the Class Members Against All Defendants

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

187. Plaintiff brings this cause of action individually and on behalf of the members of the proposed Class against Defendant.

188. Article I, Section 1 of the California Constitution guarantees each individual an inalienable right to privacy. This constitutional provision supports a private right of action against both governmental and private actors who engage in conduct that constitutes a serious invasion of privacy.

189. Plaintiff and the Class Members possess a legally protected privacy interest in the confidentiality of their online behavior, communications metadata, and identifying information, including but not limited to: IP address, browser details, session identifiers, page visit patterns, and clickstream behavior.

190. Plaintiff and the Class Members had a reasonable expectation that their activity on Defendant's website, including what pages were visited, what content was interacted with, and when, would not be secretly tracked and transmitted to third parties via embedded surveillance code.

191. Without Plaintiff's or the Class Members' knowledge or consent, Defendant caused the Trackers to be deployed on the Website. The Trackers secretly transmitted Plaintiff's digital signaling data, addressing information (e.g., URLs accessed), and routing metadata (e.g., timestamps and referral paths) to the Third Parties, enabling behavioral profiling and cross-site identification.

192. Defendant's conduct constitutes a serious and egregious invasion of Plaintiff's and the Class Members' informational privacy, far exceeding any routine or incidental data handling. The deployment of real-time surveillance tools designed to accomplish identity resolution and behavioral mapping is highly offensive to a reasonable person.

193. Defendant lacked any legitimate justification for failing to disclose or obtain consent for this data interception and transfer. The magnitude of the privacy intrusion outweighed any speculative or commercial benefit to Defendant.

194. As a direct and proximate result of Defendant's actions, Plaintiff and the Class Members have suffered a loss of control over personal data, emotional distress, and a violation of their constitutional right to privacy.

IX. THIRD CAUSE OF ACTION

Violations of Business & Professions Code § 17200

By Plaintiff and the Class Members Against All Defendants

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

196. Plaintiff brings this cause of action individually and on behalf of the members of the proposed Class against Defendant.

197. 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.

198. Defendant has engaged in unlawful business practices by:

(a) Violating Article I, Section 1 of the California Constitution, which protects individuals from serious invasions of privacy; and

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

199. 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.

200. 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.

201. 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.

202. 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.

203. 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.

X. FOURTH CAUSE OF ACTION

Intrusion Upon Seclusion

By Plaintiff and the Class Members Against All Defendants

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

205. Plaintiff brings this cause of action individually and on behalf of the members of the proposed Class against Defendant for intrusion upon seclusion, a well-established common law tort recognized in California, which protects individuals from intentional invasions of their private affairs in a manner that would be highly offensive to a reasonable person.

206. At all relevant times, Plaintiff and the Class Members had a reasonable

expectation of privacy in their online browsing activity, including their interactions with the Website, the specific content viewed, and the behavioral signals generated through use of the website, such as page views, click paths, session timestamps, and form entries.

207. Without Plaintiff's or Class Members' knowledge or consent, Defendant intentionally deployed the Trackers on the Website. This tool was engineered to surreptitiously capture and transmit granular behavioral data, including addressing, signaling, and routing information such as IP addresses, URL paths, referrers, device attributes, and mouse activity, to third parties.

208. The data collected was detailed and persistent, enabling Third Parties to monitor Plaintiff's and Class Members' conduct across websites, associate that behavior with unique identifiers, and build a behavioral profile of Plaintiff and Class Members for marketing and data monetization purposes.

209. Defendant's actions were intentional, systematic, and designed to operate in a manner undetectable by users. At no point did Defendant provide clear, conspicuous disclosure of this surveillance, nor did it obtain affirmative consent from Plaintiff and Class Members to conduct such monitoring or transmit the collected data to third parties.

210. The nature of this covert surveillance, especially its capacity to link online activity to identifiable users, would be highly offensive to a reasonable person, particularly in light of growing public sensitivity to privacy rights and digital surveillance.

211. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class Members suffered an invasion of privacy, loss of control over personal information, and emotional harm, including anxiety, indignity, and concern over being unknowingly tracked, profiled, and exposed to targeted advertising based on private digital conduct.

212. Defendant's conduct was willful, malicious, and oppressive, thereby justifying the imposition of punitive and exemplary damages.

/ / /

XI. FIFTH CAUSE OF ACTION

Unjust Enrichment

By Plaintiff and the Class Members Against All Defendants

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

214. Plaintiff brings this cause of action individually and on behalf of the members of the proposed Class against Defendant for unjust enrichment, asserting that Defendant has been unjustly enriched through the unauthorized and uncompensated acquisition, use, and monetization of Plaintiff's and Class Members' personal data.

215. Plaintiff and the Class Members, while visiting and interacting with the Website, unknowingly conferred a substantial benefit on Defendant by generating digital behavioral data, including but not limited to IP address, device information, browser metadata, URL paths, session timestamps, and interaction signals.

216. Defendant deployed the Trackers without Plaintiff's and Class Members' knowledge or meaningful consent. The data collected was then used by Defendant and/or third parties to conduct behavioral targeting, analytics, and advertising optimization that generated substantial financial value.

217. At no time did Plaintiff and Class Members consent to the commercial exploitation of this data. Nor was Plaintiff and Class Members informed that their online behavior would be tracked and monetized in this manner. Plaintiff and Class Members received no compensation, disclosure, or opportunity to prevent the enrichment conferred upon Defendant.

218. Defendant's retention and use of this benefit was unjust and inequitable. The value of Plaintiff's and Class Members' behavioral data, when compiled, analyzed, and integrated into advertising algorithms or consumer profiling tools, constitutes a marketable asset in the digital economy. Defendant's ability to extract revenue from this asset without disclosure or fair exchange renders its conduct unjust.

219. Under principles of equity and good conscience, Defendant should be

required to disgorge all ill-gotten gains and benefits received as a result of its unjust enrichment at Plaintiff's and Class Members' expense.

XII. PRAYER FOR RELIEF

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, the California Constitution, and Business & Professions Code § 17200;
3. An order declaring that Defendant's conduct unlawfully intrudes upon the seclusion of Plaintiff and the Class Members;
4. An order of judgment in favor of Plaintiff and the Class against Defendant on the cause of action asserted herein;
5. An order enjoining Defendant's conduct as alleged herein;
6. Disgorgement of profits resulting from unjust enrichment;
7. Statutory damages pursuant to CIPA;
8. Prejudgment interest;
9. Reasonable attorney's fees and costs; and
10. 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 causes of action and issues so triable.

Respectfully submitted,

Dated: January 5, 2026

NATHAN & ASSOCIATES, APC

By: */s/ Reuben D. Nathan*

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

LAW OFFICES OF ROSS CORNELL, APC
Ross Cornell, Esq. (SBN 210413)
P.O. Box 1989 #305
Big Bear Lake, CA 92315
Office: (562) 612-1708
Email: rc@rosscornelllaw.com

Attorneys for Plaintiff and the Putative Class