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: PETER DAWIDZIK

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

PETER DAWIDZIK, on behalf of himself and all similarly situated persons,

Plaintiff,

v.

TESLA, INC., a Texas corporation,

Defendant.

Case No:

COMPLAINT

1. Cal. Penal Code § 638.51
2. Cal. Bus. & Prof. Code § 17200, *et seq.*

CLASS ACTION

I. NATURE OF THE ACTION

1. Defendant TESLA, INC., a Texas corporation, (referred to herein as "Defendant" or "TESLA") own and operate a website, www.tesla.com (the "Website").

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

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

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

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

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

- Google Ads / DoubleClick Tracker
- Twitter Tracker
- Optimizely Tracker

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

8. The Trackers are operated by distinct third parties: Google LLC (Google Ads / DoubleClick Tracker); X Corp. (Twitter Tracker); and Optimizely, Inc. (Optimizely Tracker) (collectively the "Third Parties"). Defendant enables these trackers, which transmit user data to third-party servers to identify users and support advertising, profiling, and data monetization activities.

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

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

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

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

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

/ / /

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

II. PARTIES

15. Plaintiff PETER DAWIDZIK ("Plaintiff") is a California citizen residing in San Bernardino County and has an intent to remain there. Plaintiff was in California when he visited the Website, which occurred during the class period prior to the filing of the complaint in this matter. The allegations set forth herein are based on the Website as configured when Plaintiff visited it.

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

17. TESLA is a leading U.S. technology and automotive company, recognized for its electric vehicles, energy storage solutions, and clean energy products. Headquartered in Austin, Texas, TESLA maintains a broad national and international presence. The company enables individuals and businesses to explore, customize, and order vehicles, manage accounts, schedule service appointments, and access support services through its primary consumer platform at www.tesla.com.

18. TESLA operates as the flagship brand within its broader ecosystem of automotive, energy, and technology offerings. While the company provides a diverse range of products and services, the TESLA platform is directly responsible for facilitating vehicle configuration, order processing, payment management, and communications with customers. In managing its digital operations, TESLA collects and processes substantial amounts of user data for functions such as order fulfillment, user support, behavioral profiling, and targeted marketing.

19. The Website serves as TESLA's primary digital touchpoint for customers. It allows users to research vehicles and energy products, reserve orders, schedule services, and access account management. In addition to these core features, the Website also functions as a data collection and advertising platform. Through the

deployment of third-party tracking mechanisms including but not limited to the Trackers, TESLA gathers detailed information about user interactions with the Website. These practices are integral to TESLA's user engagement, marketing optimization, and audience analytics strategies.

III. JURISDICTION AND VENUE

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

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

22. Venue is proper in the Central District of California pursuant to 28 U.S.C. § 1391 because: (1) Defendant is authorized to conduct business in this District and has purposefully availed itself of the laws and commercial markets of the District; (2) Defendant conducts substantial and continuous business operations within this District; (3) Plaintiff resides in this District; and (4) the events and conduct giving rise to Plaintiff's claims occurred within this District.

IV. GENERAL ALLEGATIONS

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

23. Enacted in 1967, the California Invasion of Privacy Act (CIPA) is a legislative measure designed to safeguard the privacy rights of California residents by prohibiting unauthorized wiretapping and eavesdropping on private communications. The California Legislature recognized the significant threat posed by emerging

surveillance technologies, stating that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society" (Cal. Penal Code § 630).

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

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

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

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

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

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

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

/ / /

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

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

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

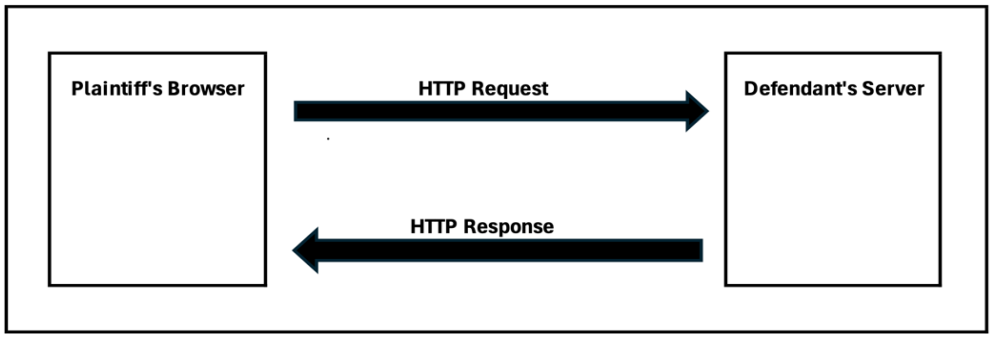
34. Individuals may pursue legal action against violators of any CIPA provision, including Section 638.51, and are entitled to seek $5,000 in statutory penalties per violation (Cal. Penal Code § 637.2(a)(1)).

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

35. When the Plaintiff and Class Members accessed the Website, their browsers initiated an HTTP or HTTPS request to Defendant's web server, which hosts the content and functionality of the site. In response, the server transmitted an HTTP response containing the necessary resources including HTML, cascading style sheets (CSS), JavaScript files, and image assets used by the browser to render and display the webpage. These resources also included client-side scripts that initiate communication

with third-party services for analytics, marketing, and tracking purposes. ***Figure 1*** below illustrates sample HTTP requests.

Figure 1



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

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

38. An Internet Protocol (IP) address is a numerical identifier assigned to each device or network connected to the Internet, used to facilitate communication between systems. *See hiQ Labs, Inc. v. LinkedIn Corp.* (9th Cir. 2019) 938 F.3d 985, 991 n.4. The most common format, known as IPv4, consists of four numbers separated

by periods (e.g., 191.145.132.123). IP addresses enable routing of data between devices and can be used via external geolocation services to infer a user's general location, including state, city, and in some cases, ZIP code.

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

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

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

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

43. As "routing, addressing, or signaling information," a public IP address is indispensable for maintaining seamless and efficient communication over the Internet.

It ensures that data packets are sent from the user's router to the intended destination, such as a website or email server.

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

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

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

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

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

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

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

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

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

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

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

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

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

55. Extracted personal data can be used to design products, platforms, and marketing techniques. A study by the McKinsey global consultancy concluded that businesses that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

56. In 2013, the Organization for Economic Cooperation and Development ("OECD") estimated that data trafficking markets had begun pricing personal data, including those obtained in illicit ways without personal consent. It found that illegal markets in personal data valued each credit cardholder record at between 1 and 30 U.S. dollars in 2009, while bank account records were valued at up to 850 U.S. dollars. Data brokers sell customer profiles of the sort that an online retailer might collect and

---

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

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

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

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

maintain for about 55 U.S. dollars, and that individual points of personal data ranged in price from $0.50 cents for an address, $2 for a birthday, $8 for a social security number, $3 for a driver's license number, and $35 for a military record (which includes a birth date, an identification number, a career assignment, height, weight, and other information). Experiments asking individuals in the United States and elsewhere how much they value their personal data points result in estimates of up to $6 for purchasing activity, and $150-240 per credit card number or social security number.[5]

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

58. The Defendant's monetization of personal data constitutes actionable economic harm under federal law, even without evidence of a direct financial loss, as a "misappropriation-like injury" caused by converting user data into a revenue stream through targeted advertising. *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020).

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

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

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

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

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

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

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

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

63. When users' data is collected without meaningful consent and monetized, they lose control over who can access, use, or distribute their personal information. Data

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

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

64. When a user visits the Website, a suite of background tracking technologies including client side scripts deployed by Google Ads / DoubleClick Tracker, Twitter Tracker, and Optimizely Tracker is activated immediately upon page load. These trackers begin collecting various categories of user information without any visible indication to the user. Together, they form a coordinated data collection infrastructure enabling TESLA to analyze user behavior at a granular level and leverage those insights in real time for marketing optimization, user targeting, and business intelligence.

65. On information and belief, these trackers operate as components of a vast and interconnected digital advertising ecosystem. By using shared identifiers, cookie syncing, and cross device tracking techniques, Google Ads / DoubleClick Tracker and Twitter Tracker can follow users across different websites and platforms. These tools are engineered to build persistent consumer profiles and support real time behavioral targeting and identity resolution on a large scale.

66. On the Website, a coordinated network comprised of third party trackers, including Google Ads / DoubleClick Tracker, Twitter Tracker, and Optimizely Tracker is deployed to facilitate identity resolution, targeted advertising, and data monetization. Some trackers, such as Google Ads / DoubleClick Tracker, may be embedded directly in the page's HTML and activate immediately upon page load, while others like Optimizely may be deployed through JavaScript execution during runtime. These

technologies work together to collect and transmit data regarding user interactions in real time, driving downstream advertising, profiling, and data sharing processes.

67. Identity resolution on the Website is primarily accomplished through the interaction of Google Ads / DoubleClick Tracker and Twitter Tracker. Google Ads / DoubleClick Tracker correlates on site activity with existing Google identifiers and advertising cookies, while Twitter Tracker links browsing behaviors to user profiles across the Twitter platform. Optimizely Tracker manages data flows and supports segmentation and audience matching. Used together, these technologies enable TESLA to associate anonymous user activity with persistent identities over time, constructing detailed behavioral and demographic user profiles.

68. Once identity signals have been captured, targeted advertising and data monetization are managed through platforms like Google Ads / DoubleClick Tracker and Twitter Tracker. These platforms engage in real time bidding and programmatic advertising, allowing TESLA to auction ad access to users based on behavioral and identity linked data. Google Ads / DoubleClick Tracker delivers performance based advertising using browsing history and user profiles, while Twitter Tracker facilitates cross channel targeting and remarketing. Collectively, these trackers transform user interactions into marketable audience segments, maximizing the effectiveness and monetization of digital marketing efforts for TESLA.

69. TESLA shares user information with third party advertising platforms, including those operated by Google and Twitter. These platforms employ real time auction systems that sell ad space to the highest bidder leveraging behavioral data collected during a user's Website visit. Data including IP address, browser type, device data, and page URLs is transmitted immediately upon page load, often without user action or explicit consent. This information allows advertisers to track users across the internet, construct behavioral profiles, and deliver personalized ads in real time.

70. Requests to Google Ads, Twitter, Optimizely, and other trackers' servers demonstrate TESLA's integration within an advertising architecture built to support real

time ad placement and behavioral targeting. By embedding immediate and silent tracking functions on page load, TESLA treats personal data as a monetizable asset, deploying these tools primarily to maximize advertising revenue and marketing performance rather than to provide functional benefits to users.

V. SPECIFIC ALLEGATIONS

1. Google Ads / DoubleClick Tracker

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

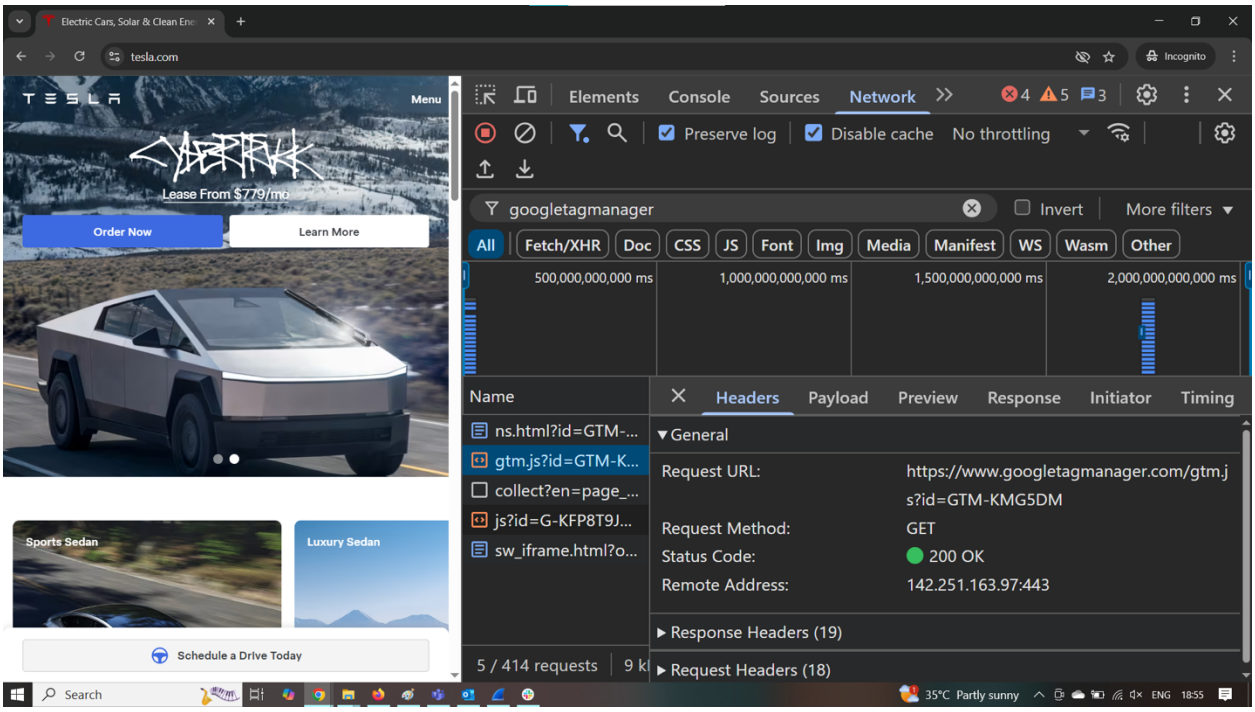
72. When implemented on the Website, the Google Ads / DoubleClick Tracker collects a broad set of user metadata, including visited URLs, session timestamps, referrer headers, and in-page activity data such as page views and navigation events. It also captures technical device attributes such as IP address,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

73. The Google Ads / DoubleClick Tracker facilitates monitoring of user activity on the Website, including the capture of pageview events and other engagement signals that can be used to track user progression through various transactional flows. These interaction signals are transmitted to Google's ad infrastructure to facilitate targeted advertising, audience retargeting, and conversion tracking. The Google Ads /

DoubleClick Tracker executes via JavaScript calls to domains including googleads.g.doubleclick.net and activates automatically upon page load without requiring any action by the user.

74. The following figures [***Figure 2*** and ***Figure 3***] provide technical evidence of the Google Ads / DoubleClick Tracker being automatically activated during a user's visit to the Website. Each screenshot evidences network activity triggered by scripts embedded in the page source, resulting in HTTP or DNS requests to external tracking domains. These network events occurred without any user interaction, confirming that the tracking technologies were operating silently in the background.

Figure 2

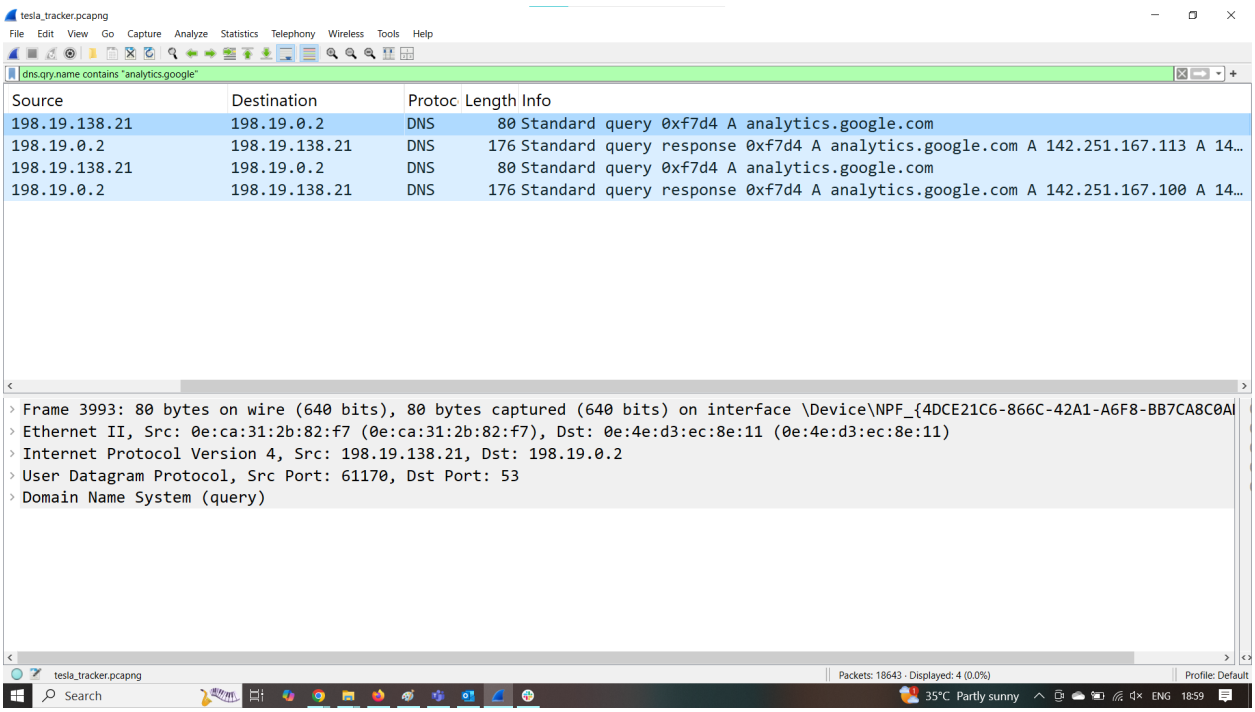


/ / /

/ / /

/ / /

Figure 3



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

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

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

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

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

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

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

2. The Twitter Tracker

81. The Twitter Tracker is a behavioral tracking script implemented through Twitter's platform technology, commonly delivered via domains such as analytics.twitter.com, syndication.twitter.com, and ads.twitter.com. On the Website, the Twitter Tracker is injected using tag management or embedded script infrastructure. Once loaded, it initiates background communication with Twitter's servers and enables real-time tracking of user activity.

82. On the Website's homepage, the Twitter Tracker activates automatically upon page load and immediately begins capturing behavioral data in real time. It records signals such as page views and other engagement events without requiring any user action. The Twitter Tracker continuously detects and collects further user interactions, including clicks and scroll actions. These signals are transmitted to Twitter's servers and may be associated with the user's Twitter profile, even if the user never directly interacts with Twitter services while on the Website.

83. The data collected by the Twitter Tracker enables identity resolution by linking behavioral information from the Website with individual user profiles across

Twitter's ecosystem. If the user is logged into Twitter on the same device or browser, the Twitter Tracker can tie Website activity to the user's unique Twitter account. Even if the user is not logged in, Twitter can assign persistent device- or browser-based identifiers using cookies, browser fingerprinting, or pixel fire events. This makes it possible to construct extensive cross-site behavioral profiles based on the user's Website activity.

84. The Twitter Tracker also advances Defendant's targeted advertising objectives by facilitating the creation of custom audience segments, groups of users who have performed certain actions on the Website, such as viewing vehicle listings, exploring product features, or starting a purchase process. Defendant can utilize Twitter's Ads Manager to re-target these users on the Twitter platform, or to create "Lookalike Audiences" that reflect the behavioral traits of the Website's visitors. These tools allow Defendant to deliver marketing messages to users most likely to respond or convert.

85. The Twitter Tracker contributes to Defendant's data monetization strategy by translating behavioral insights into quantifiable advertising results. It produces real-time analytics about user engagement, campaign effectiveness, and conversion tracking, which Twitter then reports to Defendant through its Ads infrastructure. This closed-loop system connects Website activity to off-site ad delivery, enabling Defendant to optimize ad budgets, personalize campaign content, and maximize the value of each user interaction. In this way, the Twitter Tracker operates as an integral component of Defendant's digital surveillance and marketing infrastructure.

86. The following figures [***Figure 4*** and ***Figure 5***] provide technical evidence of the Twitter Tracker being automatically activated during a user's visit to the Website. Each screenshot evidences network activity triggered by scripts embedded in the page source, resulting in HTTP or DNS requests to external tracking domains.

These network events occurred without any user interaction, confirming that the tracking technologies were operating silently in the background.

Figure 4

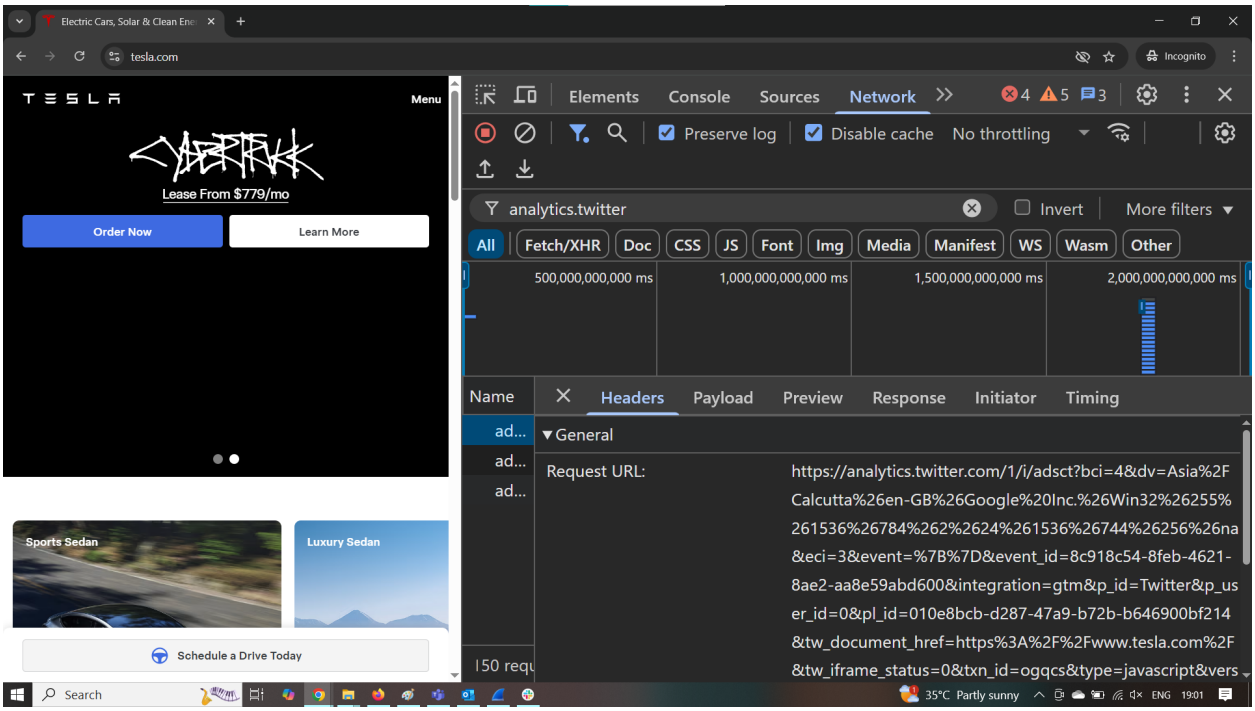
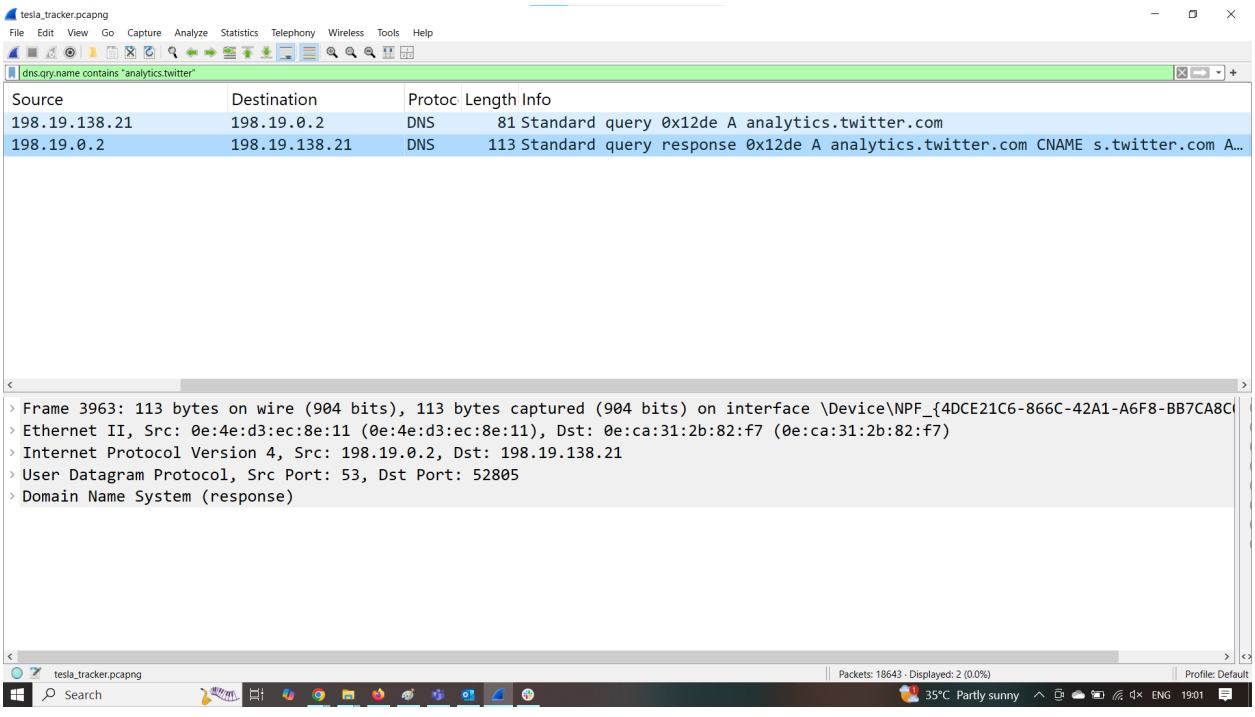


Figure 5



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

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

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

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

91. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Twitter Tracker on Plaintiff's and Class Members' browsers or to collect or share data with Twitter.

3. The Optimizely Tracker

92. The Optimizely Tracker, typically delivered through domains such as cdn.optimizely.com and related assets, is a client-side behavioral tracking and

experimentation tool operated by Optimizely, Inc. On the Website, this tracker is dynamically injected into users' browsers upon arrival. Once active, it establishes a connection to Optimizely's servers and begins collecting a range of data including IP address, browser and device specifications, geolocation, referrer URLs, and session identifiers. These data transmissions are initiated automatically and occur silently in the background, without any user interaction or consent, confirming that real-time monitoring of user behavior is occurring for testing, personalization, and audience segmentation purposes.

93. Once initialized, the Optimizely Tracker plays a critical role in user identity resolution and behavioral segmentation. It assigns users persistent identifiers and tracks their engagement with specific elements of the Website such as button clicks, page variants, form interactions, and scroll behavior. Through the use of cookies, A/B testing assignments, and internal analytics mechanisms, Optimizely builds a behavioral profile that can persist across sessions and even across multiple digital properties using consistent identifiers. These capabilities allow Optimizely to associate user behavior on the Website with broader audience attributes for personalization and targeted content delivery.

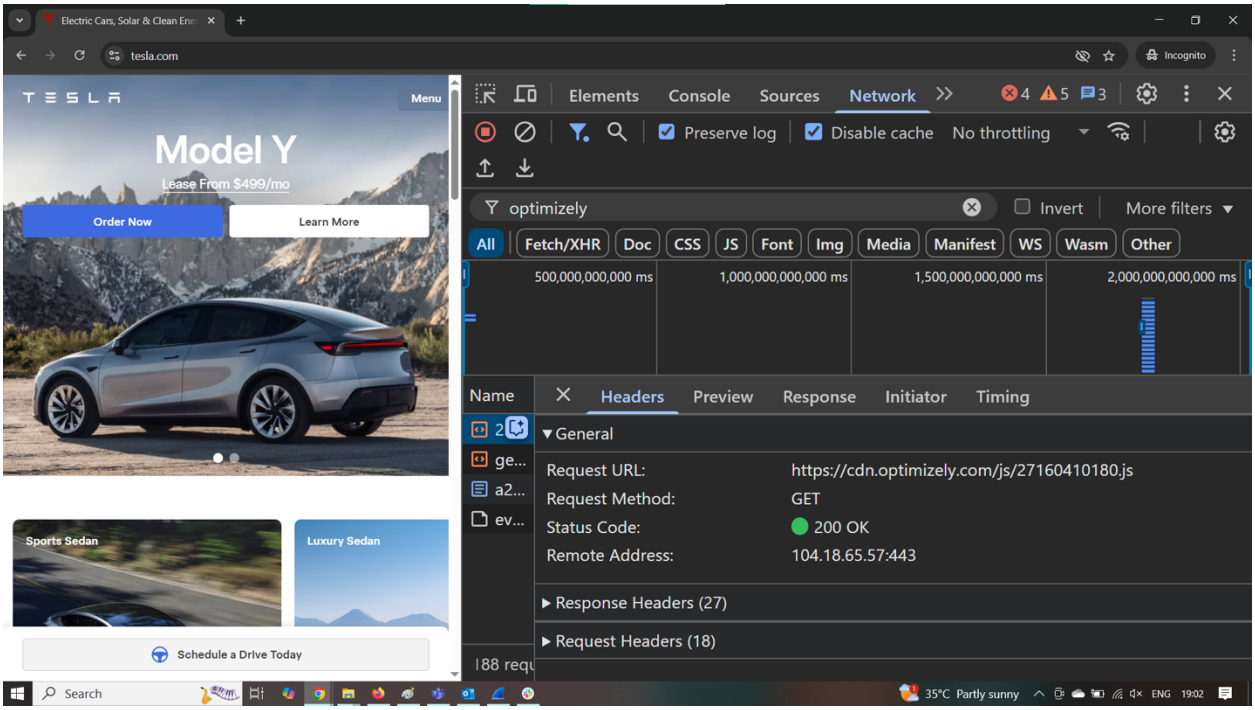
94. The Optimizely Tracker enables the Website operator to dynamically tailor user experiences and deliver targeted content or promotions based on prior user behavior. For example, visitors who interact with specific product pages, complete forms, or abandon carts may be segmented for inclusion in personalized experiments or marketing strategies. This behavioral data may also be passed downstream to integrated third-party platforms such as customer relationship management systems or advertising networks for use in remarketing campaigns, conversion attribution, and cross-channel user engagement. In this capacity, Optimizely enhances the Website's ability to retain, convert, and re-engage users with tailored digital experiences.

95. On the Website, the Optimizely Tracker converts real-time behavioral interactions into actionable experimental data that supports revenue-driven strategies.

By logging events like clicks, hovers, scrolls, and navigation behavior, Optimizely enables the site operator to run A/B and multivariate tests that optimize conversion paths, refine design elements, and maximize user engagement. The tracker also feeds data into personalization engines that adjust on-page content in real time. In doing so, Optimizely acts as a silent intermediary between user behavior and site modification, helping the Website continuously adapt to user preferences while capturing rich data for analytics, segmentation, and marketing optimization.

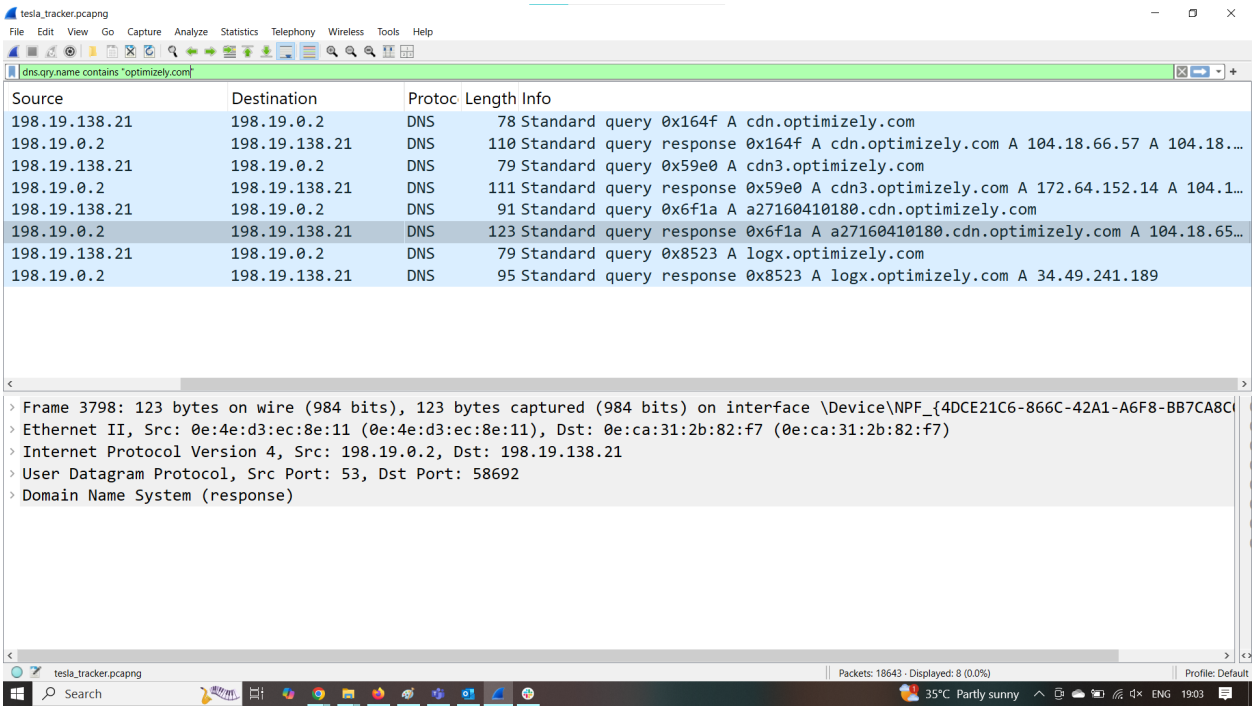
96. The following figures [***Figure 6*** and ***Figure 7***] provide technical evidence of the Optimizely Tracker being automatically activated during a user's visit to the Website. Each screenshot evidences network activity triggered by scripts embedded in the page source, resulting in HTTP or DNS requests to external tracking domains. These network events occurred without any user interaction, confirming that the tracking technologies were operating silently in the background.

Figure 6



/ / /

Figure 7



97. Defendant surreptitiously installed, executed, embedded, or injected the Optimizely Tracker onto users' browsers by deploying JavaScript code that communicates with Optimizely's behavioral experimentation infrastructure. When a user visits the Website, their browser automatically executes this script, initiating outbound requests to cdn.optimizely.comand related Optimizely domains. These requests transmit user metadata including IP address, page URL, browser characteristics, session identifiers, and experimental assignment values to Optimizely's servers. This transmission occurs silently and without any user interaction, enabling Optimizely to capture data about user behavior on the Website in real time.

98. The Optimizely Tracker qualifies at minimum as a "process" under the California Invasion of Privacy Act (CIPA), as it is software that identifies users, collects behavioral data, and correlates that data to deliver personalized experiences and experimental results.

/ / /

99. The Optimizely Tracker also constitutes a "device" because software functions only when executed on a computing device. See, e.g., *James v. Walt Disney Co.*, 2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023).

100. The Optimizely Tracker establishes a connection to its backend infrastructure automatically upon page load through the execution of client-side scripts. It collects metadata including IP address, visited URLs, timestamps, referrer headers, and experimental variation identifiers. All of this constitutes signaling and routing information under the meaning of CIPA.

101. The user does not intentionally initiate any communication with Optimizely. Instead, the connection is automatically triggered in the background by embedded third-party code. As a result, Optimizely is able to intercept and log communication-related metadata generated during a user's visit. This silent and passive operation allows the Optimizely Tracker to function as a surveillance mechanism that captures behavioral and routing signals associated with web interactions.

102. Defendant did not obtain a court order authorizing the use of a pen register or trap and trace device, nor did it obtain the express or implied consent of Plaintiffs or Class Members to install the Optimizely Tracker on their browsers or to collect, process, or transmit their data to Optimizely's systems.

103. Accordingly, Defendant's deployment of the Optimizely Tracker constitutes a violation of the California Invasion of Privacy Act (CIPA) concerning the unauthorized use of a pen register and/or trap and trace device without user consent or judicial authorization.

VI. CLASS ALLEGATIONS

104. 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.

105. **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.

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

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

107. **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.

/ / /

108. **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.

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

VII. FIRST CAUSE OF ACTION

Violations of Cal. Penal Code § 638.51

By Plaintiff and the Class Members Against All Defendants

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

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

112. 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.

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

/ / /

VIII. SECOND CAUSE OF ACTION

Violations of Business & Professions Code § 17200

By Plaintiff and the Class Members Against All Defendants

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

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

116. 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.

117. Defendant has engaged in unlawful business practices by:

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

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

118. 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.

119. 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.

120. 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.

121. 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.

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

IX. 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 and Business & Professions Code § 17200;
3. An order of judgment in favor of Plaintiff and the Class against Defendant on the causes of action asserted herein;

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

DEMAND FOR JURY TRIAL

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

Dated: July 31, 2025

NATHAN & ASSOCIATES, APC

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