

1 Reuben D. Nathan, Esq. (SBN 208436)
2 **NATHAN & ASSOCIATES, APC**
3 2901 W. Coast Hwy., Suite 200
4 Newport Beach, CA 92663
5 Office: (949) 270-2798
6 Email: rnathan@nathanlawpractice.com

7 Ross Cornell, Esq. (SBN 210413)
8 **LAW OFFICES OF ROSS CORNELL, APC**
9 40729 Village Dr., Suite 8 - 1989
10 Big Bear Lake, CA 92315
11 Office: (562) 612-1708
12 Email: rc@rosscornelllaw.com

13 Attorneys for Plaintiff: PETER DAWIDZIK

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

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

19 Plaintiff,

20 v.

21 TESLA, INC., a Texas corporation,

22 Defendant.

Case No:

COMPLAINT

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

CLASS ACTION

1 **I. NATURE OF THE ACTION**

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

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

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

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

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

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

- 21 • Google Ads / DoubleClick Tracker
- 22 • Twitter Tracker
- 23 • Optimizely Tracker

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

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

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

12 10. Because the Trackers capture and transmit users' IP addresses, full page
13 URLs, referrer headers, device identifiers, and other non-content metadata, they
14 function as "pen registers" and/or "trap and trace devices" under Cal. Penal Code §
15 638.50. These tools silently collect routing and addressing information for commercial
16 use without user interaction, as defined in *Greenley v. Kochava, Inc.*, 2023 WL 4833466
17 (S.D. Cal. July 27, 2023).

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

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

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

28 ///

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

3 **II. PARTIES**

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

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

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

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

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

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

5 **III. JURISDICTION AND VENUE**

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

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

17 22. Venue is proper in the Central District of California pursuant to 28 U.S.C.
18 § 1391 because: (1) Defendant is authorized to conduct business in this District and has
19 purposefully availed itself of the laws and commercial markets of the District; (2)
20 Defendant conducts substantial and continuous business operations within this District;
21 (3) Plaintiff resides in this District; and (4) the events and conduct giving rise to
22 Plaintiff’s claims occurred within this District.

23 **IV. GENERAL ALLEGATIONS**

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

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

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

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

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

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

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

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

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

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

28 ///

1
2 31. Despite predating the Internet, CIPA has been interpreted by the
3 California Supreme Court to apply to new technologies where such application does not
4 conflict with the statutory scheme (*In re Google Inc.*, 2013 WL 5423918, at *21;
5 *Greenley*, supra, 2023 WL 4833466, at *15; *Javier v. Assurance IQ, LLC*, 2022 WL
6 1744107, at *1). This interpretation aligns with the principle that CIPA should be
7 construed to provide the greatest privacy protection when faced with multiple possible
8 interpretations (*Matera v. Google Inc.*, 2016 WL 8200619, at *19).

9 32. The conduct alleged herein constitutes a violation of a legally protected
10 privacy interest that is both concrete and particularized. Invasions of privacy have long
11 been actionable under common law. (*Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir.
12 2019); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017).)

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

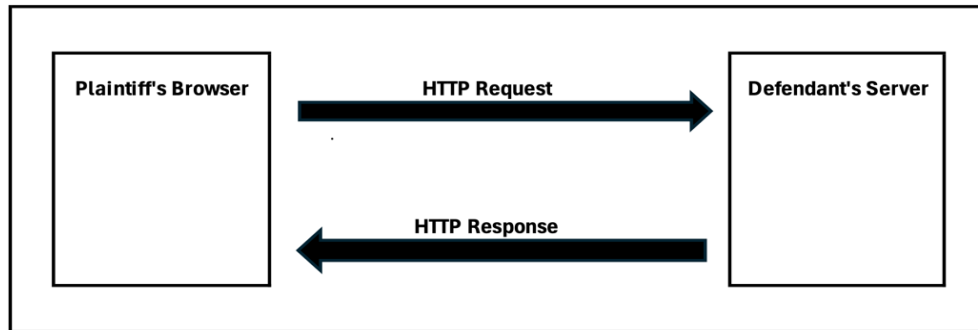
18 34. Individuals may pursue legal action against violators of any CIPA
19 provision, including Section 638.51, and are entitled to seek \$5,000 in statutory
20 penalties per violation (Cal. Penal Code § 637.2(a)(1)).

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

22 35. When the Plaintiff and Class Members accessed the Website, their
23 browsers initiated an HTTP or HTTPS request to Defendant’s web server, which hosts
24 the content and functionality of the site. In response, the server transmitted an HTTP
25 response containing the necessary resources including HTML, cascading style sheets
26 (CSS), JavaScript files, and image assets used by the browser to render and display the
27 webpage. These resources also included client-side scripts that initiate communication
28

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

3 *Figure 1*



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

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

25 38. An Internet Protocol (IP) address is a numerical identifier assigned to
26 each device or network connected to the Internet, used to facilitate communication
27 between systems. *See hiQ Labs, Inc. v. LinkedIn Corp.* (9th Cir. 2019) 938 F.3d 985,
28 991 n.4. The most common format, known as IPv4, consists of four numbers separated

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2 52. Given the number of Internet users, the “world’s most valuable resource
3 is no longer oil, but data.”¹

4 53. Consumers’ web browsing histories have an economic value more than
5 \$52 per year, while their contact information is worth at least \$4.20 per year, and their
6 demographic information is worth at least \$3.00 per year.²

7 54. There is “a study that values users’ browsing histories at \$52 per year, as
8 well as research panels that pay participants for access to their browsing histories.”³

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

13 56. In 2013, the Organization for Economic Cooperation and Development
14 (“OECD”) estimated that data trafficking markets had begun pricing personal data,
15 including those obtained in illicit ways without personal consent. It found that illegal
16 markets in personal data valued each credit cardholder record at between 1 and 30 U.S.
17 dollars in 2009, while bank account records were valued at up to 850 U.S. dollars. Data
18 brokers sell customer profiles of the sort that an online retailer might collect and
19

20 ¹ Ian Cohen, Are Web-Tracking Tools Putting Your Company at Risk?, Forbes (Oct
21 19, 2022), <https://www.forbes.com/sites/forbestechcouncil/2022/10/19/are-web-tracking-tools-putting-your-company-atrisk/?sh=26481de07444>

22 ² *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 928 (N.D. Cal.
23 2015), rev’d, 956 F.3d 589 (9th Cir. 2020).

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

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

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

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

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

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

18 59. Data harvesting is one of the fastest growing industries in the country,
19 with estimates suggesting that internet companies earned \$202 per American user in
20 2018 from mining and selling data. That figure is expected to increase with estimates
21 for 2022 as high as \$434 per use, reflecting a more than \$200 billion industry.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 **V. SPECIFIC ALLEGATIONS**

6 ***1. Google Ads / DoubleClick Tracker***

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

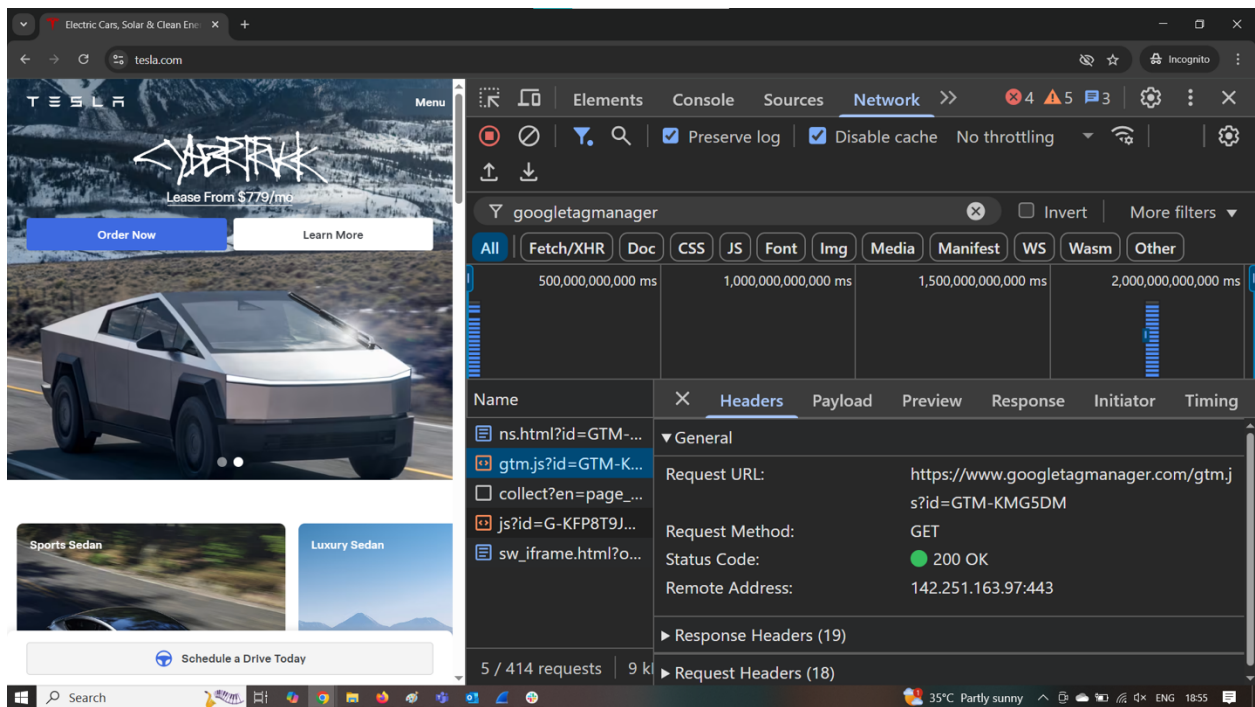
13 72. When implemented on the Website, the Google Ads / DoubleClick
14 Tracker collects a broad set of user metadata, including visited URLs, session
15 timestamps, referrer headers, and in-page activity data such as page views and
16 navigation events. It also captures technical device attributes such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

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

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

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

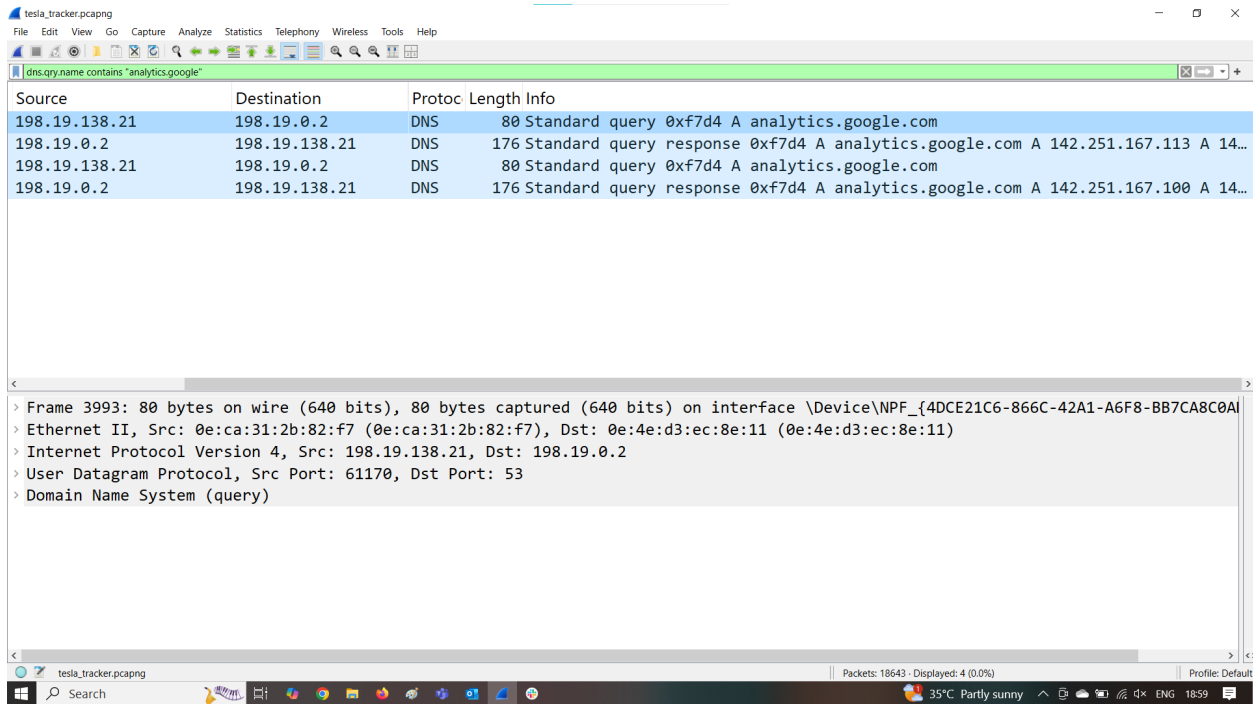
10 *Figure 2*



23 ///

24 ///

25 ///

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

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

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

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

13 **2. *The Twitter Tracker***

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

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

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

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

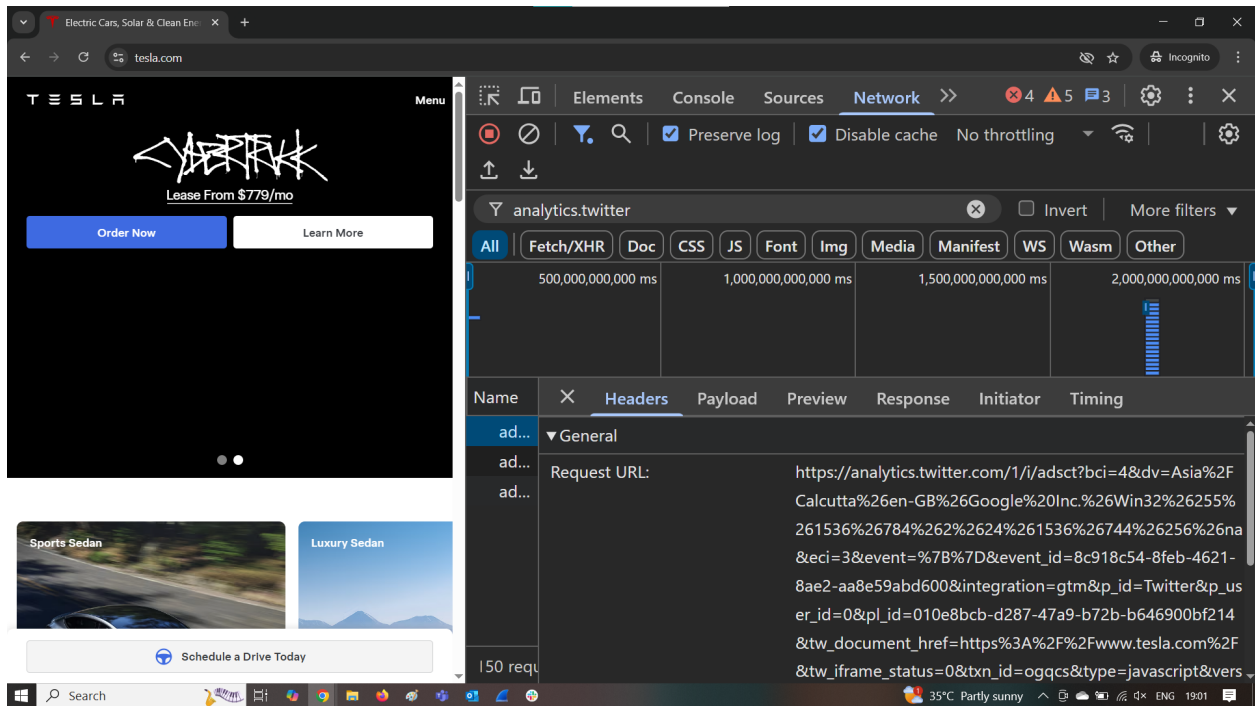
7 84. The Twitter Tracker also advances Defendant's targeted advertising
8 objectives by facilitating the creation of custom audience segments, groups of users who
9 have performed certain actions on the Website, such as viewing vehicle listings,
10 exploring product features, or starting a purchase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

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

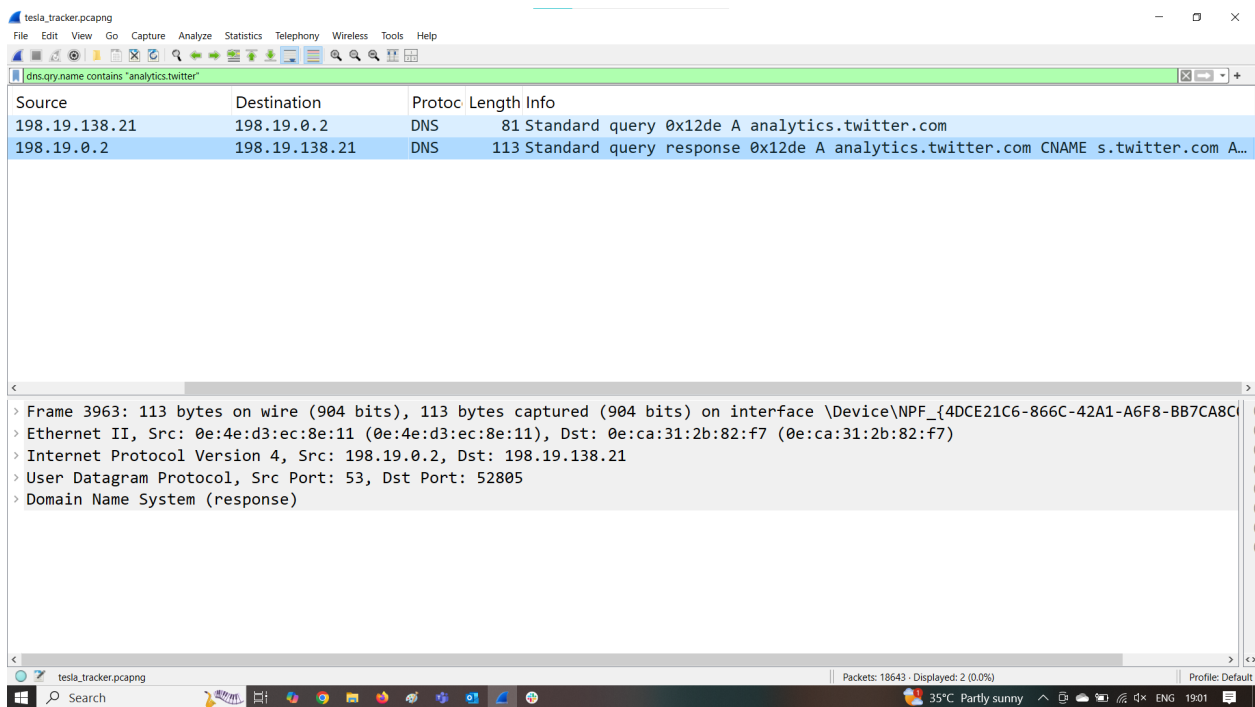
24 86. The following figures [*Figure 4* and *Figure 5*] provide technical
25 evidence of the Twitter Tracker being automatically activated during a user's visit to
26 the Website. Each screenshot evidences network activity triggered by scripts embedded
27 in the page source, resulting in HTTP or DNS requests to external tracking domains.
28

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

3 *Figure 4*



15
16
17 *Figure 5*



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

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

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

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

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

26 **3. *The Optimizely Tracker***

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

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

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

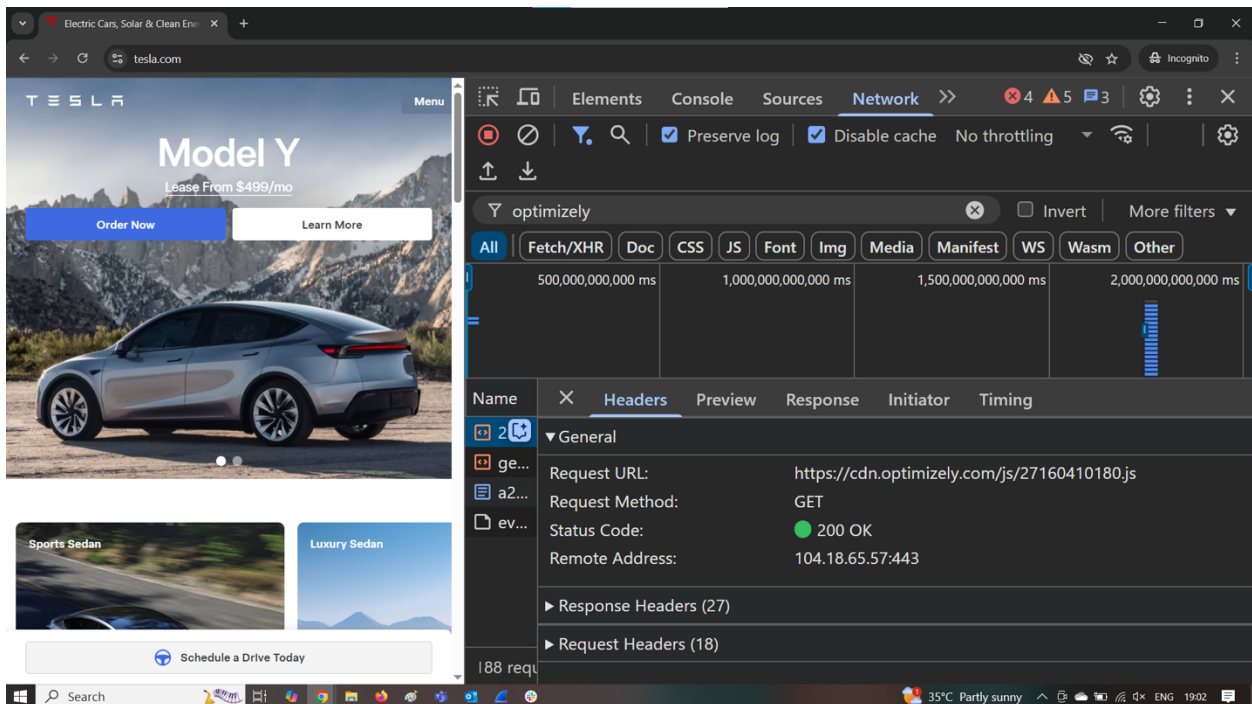
18 94. The Optimizely Tracker enables the Website operator to dynamically
19 tailor user experiences and deliver targeted content or promotions based on prior user
20 behavior. For example, visitors who interact with specific product pages, complete
21 forms, or abandon carts may be segmented for inclusion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

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

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

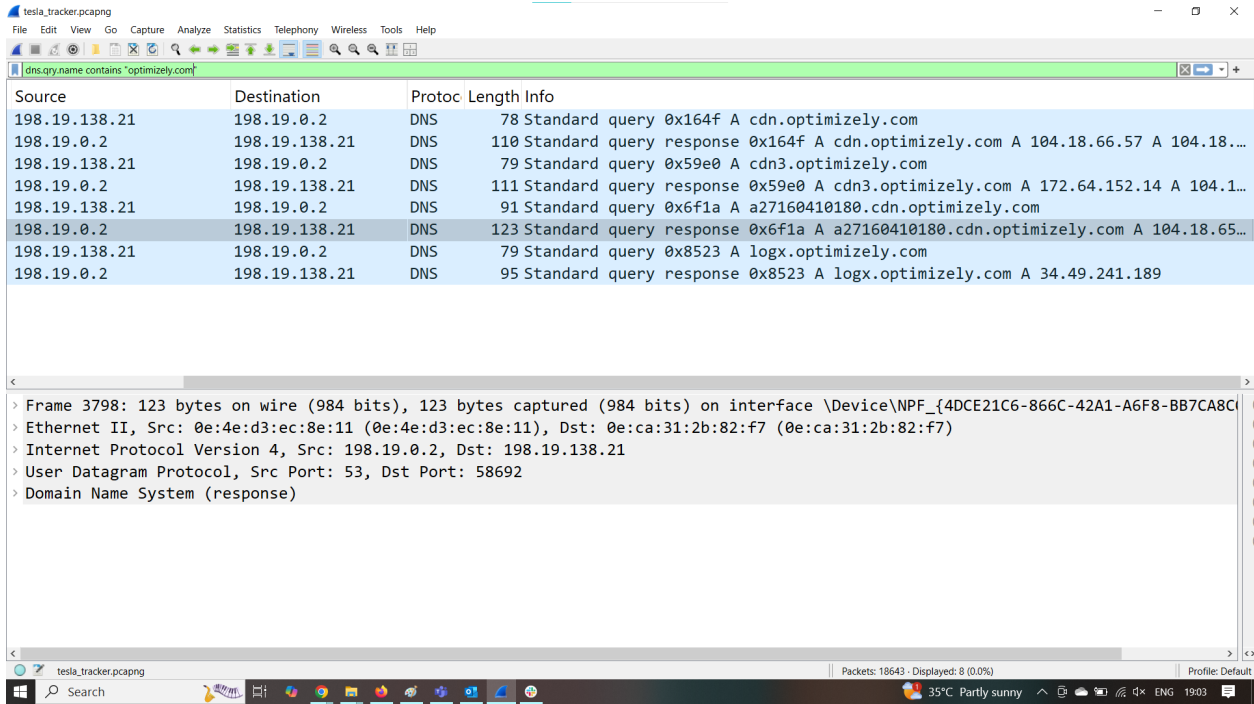
8 96. The following figures [*Figure 6* and *Figure 7*] provide technical
9 evidence of the Optimizely Tracker being automatically activated during a user's visit
10 to the Website. Each screenshot evidences network activity triggered by scripts
11 embedded in the page source, resulting in HTTP or DNS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

14 *Figure 6*



28 ///

Figure 7



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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.com and 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.

///

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

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

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

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

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

23 VI. CLASS ALLEGATIONS

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

26 All persons within California whose browser was subject to
27 installation, execution, embedding, or injection of the Trackers by
28

1 the Defendant's Website during the relevant statute of limitations
2 period.

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

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

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

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

28 ///

1 108. **ADEQUACY:** Plaintiff will fairly and adequately protect the interests
2 of the members of the Class. Plaintiff has retained attorneys experienced in class action
3 litigation. All individuals with interests that are actually or potentially adverse to or in
4 conflict with the Class or whose inclusion would otherwise be improper are excluded.

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

10 **VII. FIRST CAUSE OF ACTION**

11 **Violations of Cal. Penal Code § 638.51**

12 ***By Plaintiff and the Class Members Against All Defendants***

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

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

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

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

28 ///

1 **VIII. SECOND CAUSE OF ACTION**

2 **Violations of Business & Professions Code § 17200**

3 ***By Plaintiff and the Class Members Against All Defendants***

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

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

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

11 117. Defendant has engaged in unlawful business practices by:

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

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

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

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

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

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

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

21 **IX. PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiff prays for the following:

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

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

6 **DEMAND FOR JURY TRIAL**

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

8

9 Dated: July 31, 2025

NATHAN & ASSOCIATES, APC

10

11 By: /s/ Reuben D. Nathan

12 Reuben D. Nathan, Esq.

13 Attorneys for Plaintiff

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Lawsuit Claims Third-Party Trackers on Tesla Website Collect User Data Without Consent](#)
