

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

CAROL PRICE, individually and on behalf
of all others similarly situated,

Plaintiff,

vs.

WEWORK INC., a Delaware corporation;
and DOES 1 through 10, inclusive,

Defendants.

Case No.

**CLASS ACTION COMPLAINT FOR
(1) USE OF A TRAP AND TRACE
DEVICE IN VIOLATION OF THE
CALIFORNIA INVASION OF
PRIVACY ACT (CAL. PENAL CODE §
638.51); (2) INTRUSION UPON
SECLUSION**

INTRODUCTION

1. Plaintiff, on her behalf and on behalf of a class of similarly situated persons, brings this action against Defendant WeWork Inc. (“Defendant” or “WeWork”). WeWork markets “workspace solutions” such as renting desks and office spaces at co-working locations through its website, found at <https://wework.com/> (the “Website”).

2. Defendant has installed and deployed software developed by a California-registered data broker, LiveRamp Holdings, Inc. (“LiveRamp”), on the Website to secretly collect data about visitors, their devices, locations and views of webpages to identify who they are, target them with unwanted marketing and track them on an ongoing basis.

3. The data broker software identifies visitors based on the data collected from visitors’ devices and browsers, sometimes linking the data received to data already in the possession of data brokers, such as email addresses, physical addresses and name.

4. Both Defendant and LiveRamp benefit commercially and financially from this activity. They benefit because collected visitor data, and the identification of visitors using that data, are used to, among other things, target Website visitors for specific marketing. LiveRamp benefits because it uses the data to, *inter alia*, compile more comprehensive profiles of visitors, which it may sell to third parties for advertising and other purposes.

5. Defendant’s installation and use of data broker software without obtaining consent

or authorization therefore violated California Penal Code § 638.51, California's Trap and Trace Law, and duties Defendant owed to Plaintiff and other visitors to the Website similarly situated to her under applicable common law.

JURISDICTION AND VENUE

6. 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.

7. This Court has general jurisdiction over Defendant WeWork, a Delaware corporation, because its principal offices are located in New York, New York.

8. Venue is proper in the Southern District of New York pursuant to 28 U.S.C. § 1391 because Defendant resides in the District, where it maintains its principal offices.

PARTIES

9. Plaintiff Carol Price ("Plaintiff") is, and at all times relevant to this complaint has been, a citizen of California. Plaintiff maintains reasonable expectations of privacy when browsing websites.

10. Defendant is a Delaware corporation, headquartered in New York, New York, that leases office space to individual proprietors and businesses.

11. Plaintiff identifies DOE Defendants 1 through 10 as unknown entities that Defendant directed and controlled to participate in implementing or maintaining Defendant's system. Plaintiff will seek leave to amend this Complaint to identify these entities when Defendant's discovery responses reveal their true names and roles.

12. Each DOE Defendant acted as Defendant's agent or employee in Defendant's implementation of the surveillance scheme described herein. Each DOE Defendant operated within the scope of its relationship with Defendant and participated with Defendant in the common plan to unlawfully track California residents for Defendant's commercial gain.

FACTUAL ALLEGATIONS

13. Defendant owns and operates the Website.

14. On October 5, 2025, Plaintiff visited the Website. When she did, data that identified her were transmitted to at least one third party who used and profited from that data, along with Defendant, LiveRamp. This occurred through the operation of software and code on the Website.

Defendant Shares Visitors' Data with at least 3 Data Brokers

15. Defendant has partnered with at least one registered California data broker, LiveRamp, in order to deanonymize and develop clandestine user profiles on otherwise anonymous website visitors. Defendant has done this by installing code and tools proprietary to LiveRamp on the Website.

16. The code supplied by LiveRamp (the "Data Broker Code") is designed to track and correlate visitors by capturing electronic impulses transmitted from the devices of visitors to a website on which it is deployed. The process initiated by the Data Broker Code identifies visitors through "browser fingerprinting." Fingerprinting allows data brokers like LiveRamp to ascertain the identity of a website visitor by plotting hundreds of personal identifiers, including a user's geolocation, device information, identification and cross-referencing of tracking cookies installed on their devices, and other traits evident from a user's browser.

Browser Fingerprinting

17. Why does it matter that data about a Website visitor such as the size of her screen, her device's brand name and her browser settings get transmitted to LiveRamp? One would think that the sharing of such seemingly non-personal data cannot impact a visitor's life or experience. This assumption is simply incorrect.

18. The fact is that when you visit a website, ***and before you get to weigh in on whether you should be targeted with ads or identified***, hundreds of non-personal data points tell LiveRamp who you are. (These data points are *usually* accompanied with information such as the webpage you viewed just prior to arrival, and geolocation data.) LiveRamp may already have access to your

name and email addresses, as well as other websites you have visited in the past, to combine and/or match with this incoming data from your device.

19. Examples of such non-personal data points are:

- Device type and configuration
- Browser type and version
- Operating system and version
- Screen resolution and color depth
- System language settings
- Time zone settings
- Installed fonts
- Installed browser plugins or extensions
- Device memory
- CPU class
- Canvas rendering characteristics
- WebGL rendering characteristics
- AudioContext processing characteristics
- Touch support and input capabilities
- Network connection type

20. To be clear, ***website operators*** require some of the data points at issue to render the contents of a page on a website on their visitors' devices. For example, a webpage will load properly on a visitor's screen only with information about a visitor's device characteristics and configurations, including screen size. What is being discussed here – and what is at issue in this action – is such data being provided, by a website operator's actions, to ***third parties involved neither in operation of the website itself nor the rendering of the website's contents on visitors' screens***. The third parties do not need the data to operate any website, or for any purpose other than to identify, profile, target and track website visitors.

21. As explained in an article in the October 2025 issue of *Wired Magazine*:

Your browser fingerprint is a collection of innocuous information about your PC that, *when put together, is unique enough that it could identify an individual*. Some of the components of your browser fingerprint include your computer's hardware, your browser and version, the various versions of software you have running in your browser, the fonts you have installed on your PC, your time zone, your system language, your keyboard layout; the list goes on. Out of the dozens of pieces of information, none of them could identify you individually. It's when this data is bundled together that your fingerprint becomes unique.¹

22. The fingerprinting process works even when a visitor does not enter any items *colloquially referred to* as “personal data” – such as name, telephone number, address or email address – into a form on a website.

23. In 2025, researchers at U.S. universities found evidence of the use of browser fingerprinting by websites, particularly in connection with advertising.² Through research, Dr. Yinzhi Cao, Associate Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University, and other scholars, have “correlate[d] browser fingerprints and ad behaviors, essentially establishing the relationship between web tracking and fingerprinting.”³

The Cycle of Third-Party Collection of Consumer Data and the Tracking of Consumers

24. Collection of visitor data by entities such as LiveRamp – including collection by

¹ Jacob Roach, “Here’s What Your Browser Is Telling Everyone About You: Your browser sends a lot of information with each website you visit. That can be used to track you across the internet.” (Wired Magazine, Oct. 16, 2025), available at <https://www.wired.com/story/what-is-browser-fingerprinting/> (last viewed 6/7/2026).

² Texas A&M Univ. Dep’t of Computer Science and Engineering, “Websites Are Tracking You Via Browser Fingerprinting: New research provides the first evidence of the use of browser fingerprints for online tracking.” (Texas A&M Stories June 26, 2025), available at <https://stories.tamu.edu/news/2025/06/26/websites-are-tracking-you-via-browser-fingerprinting/> (last viewed 7/20/2026).

³ *Id.*

these entities of unique identifiers that the Data Broker Code assigns to visitors to the websites of advertising companies like WeWork – enables ongoing tracking of website visitors as they visit new websites in the future. At the same time, the tracking of a person’s internet browsing going forward provides more opportunities for data collection (and profile building) about an individual. This cycle aids the advertising and/or data monetization efforts of LiveRamp and similar organizations.

25. As California Attorney General Rob Bonta explained in a 2022 California Superior Court complaint filed against retailer/website operator Sephora USA, Inc.:

Consumers are constantly tracked when they go online. Sephora, like many online retailers, allows third-party companies to install tracking software on its website and in its app so that these third parties can monitor consumers as they shop. The third parties track all types of data; in Sephora’s case, third parties can track whether a consumer is using a MacBook or a Dell, the brand of eyeliner that a consumer puts in their “shopping cart,” and even the precise location of the consumer. Some of these third-party companies create entire profiles of users who visit Sephora’s website, which the third parties then use for Sephora’s benefit. For example, the third party might provide detailed analytics information about Sephora’s customers and provide that to Sephora, or offer Sephora the opportunity to purchase online ads targeting specific consumers [. . .]. This data about consumers is frequently kept by companies and used for the benefit of other businesses, without the knowledge or consent of the consumer.

Complaint, *People of the State of California v. Sephora USA, Inc.*, CGC-22-601380, 2022 CA Sup. Ct. Pleadings LEXIS 38450 (Cal. Super. Ct., San Francisco Co., Aug. 24, 2022) (the “Sephora Complaint”), at 2:2-13.

Registered California Data Brokers, Including LiveRamp

26. Registered California data brokers are companies whose core business is to collect, aggregate, analyze, and sell or license personal and non-personal data about individuals and organizations. Data brokers operate largely behind the scenes, often without direct interaction with the individuals whose data they monetize.

27. Registered California data brokers gather information from a wide variety of sources, including by purchasing information from commercial sources like retailers, financial institutions, online marketplaces, subscription services, and loyalty programs.

28. Once the data is collected it is consolidated and organized into comprehensive profiles that may include thousands of attributes per individual. The data is then cross-referenced and linked using unique identifiers like device IDs and cookies to unify data about individual users from multiple sources.

29. Data brokers are accumulating data and profiling individuals to an alarming extent. As the CEO of a data broker recently described the extent of their surveillance abilities as to an otherwise anonymous individual: “We know who she is, what she watches, what she reads, and who she lives with. [We] also know who she follows on social media, what she buys online and offline, where she buys, when she buys, and more importantly, why she buys. We know that [she] has two children and that her kids drink lots of premium fruit juice. We can see that the price of the SKU she buys has been steadily rising on her local retailer’s shelf. We can also see that [her] income has not been keeping pace with inflation.”⁴

30. Given the amount of data available by way of California registered data brokers’ practices, a company like WeWork has an incentive to partner with data brokers so that it can learn the identity of visitors in order to target them with specific marketing materials.

⁴ Lucas Ropek, “Data Broker Brags About Having Highly Detailed Personal Information on Nearly All Internet Users” (Gizmodo.com March 15, 2025), available at <https://gizmodo.com/data-broker-brags-about-having-highly-detailed-personal-information-on-nearly-all-internet-users-2000575762> (last viewed 2/22/2026).

31. Here, Defendant partnered with LiveRamp by installing the Data Broker software onto the Website. Defendant allows LiveRamp, and possibly other data brokers, to access, use, and monetize the visitor data provided by Defendant, in ways that remain undisclosed to the public.

The Data Broker Code

32. LiveRamp is one of the largest data brokers in California, specializing in deanonymization of website users. The Data Broker Code on Defendant's Website tracks online signals from a website visit and matches it with their vast database to create a universal serial number for a person called a "RampID." The LiveRamp code functions as follows:

33. First, when the Data Broker Code loads on a webpage, it immediately captures the user's identifiers present in that context – e.g. reading any first-party cookie ID or a platform's ID that the page passes, as well as standard header info like IP and user-agent.

34. Second, the data obtained by the Data Broker Code is sent to LiveRamp's servers where LiveRamp combines the data obtained from a visit to Defendant's website with other data it has obtained about the individual both online and offline. This data may include name and postal address, email address, cookie IDs, and mobile device IDs.

35. Third, through this process, the user is matched with their pre-existing "RampID" (data broker serial number). LiveRamp's RampID is permanent, and designed to persistently track an individual across thousands of websites. RampIDs do not change with clearing cookies or switching devices. The RampID, and the data associated with it, is widely shared with dozens of ad tech partners so that all parties who pay for it can identify the user, and see the user's online habits.

36. Identification of website visitors through the Data Broker Code happens in "real-time," allowing the websites of LiveRamp's customers to "access people-based data immediately at the time of impression." It also works across devices: In other words, the Data Broker Code can inform websites using it that the same account or person has accessed the website from different devices. As LiveRamp explains, "[w]ith impressions matched to a persistent people-based ID, data are stitched across devices and not lost over time with new cookies or phones."

37. Plaintiff was subjected to the Data Broker Code as described *supra* starting when she requested that the Website load on her device on October 5, 2025.

Troubling Implications of Third-Party Data Sharing

38. Companies using third-party tracking software – such as the Data Broker Code described above – often seek to downplay its significance. They emphasize that the data collected by such software is being used simply to inform consumers about products they believe would be particularly appealing to them. However, there is no guarantee that consumer data supplied to data brokers or social media platforms will be used solely for advertising purposes.

39. As Attorney General Bonta explained in the *Sephora* case:

The ramifications of this third-party surveillance can go beyond ordinary consumer profiling. Sephora’s website allows visitors to browse and purchase products such as prenatal and menopause support vitamins—data points which can be used by third-party companies to infer conclusions about women’s health conditions, like pregnancy. Moreover, when a company like Sephora utilizes third-party tracking technology without alerting consumers and giving them the opportunity to control their data, they deprive consumers of the ability to limit the proliferation of their data on the web.

Sephora Complaint, at 2:14-20.

40. As a data broker, LiveRamp can use data it received regarding Plaintiff’s visit to the Website to further profile Plaintiff, with the objective of monetizing this data by selling or licensing it to other entities, including law enforcement and government agencies. The same can be said of data they received regarding visits of members of the putative Class in this action.

41. A recent report by the Brennan Center, a public policy nonprofit, has explained that “government agencies may purchase personal data to further their exercise of coercive powers, including the ability to deport, arrest, incarcerate, or even use lethal force.”⁵

42. There are recent examples of tech companies exchanging information with the federal government in ways that threaten civil liberties and individuals with minority viewpoints. For example, U.S. Immigration and Customs Enforcement (ICE) has partnered with Palantir Technologies, a Denver-based software company, to use artificial intelligence and data mining to identify, track, and deport suspected noncitizens.⁶

43. Another example of such government data exchange is the provision by Meta, pursuant to valid warrants, of user data such as Facebook messages, for the purpose of investigating and prosecuting state crimes related to abortion.⁷

44. In February 2026, Google handed over user data to the United States Department of Homeland Security (“DHS” or “Homeland Security”) based on an administrative subpoena for the investigation of an individual based on the fact that he had written to a DHS attorney advocating on behalf of a refugee from Afghanistan in deportation proceedings.⁸ No clear legal authority exists preventing the sale or dissemination of user data by Data Brokers to the federal government.

45. The New York Times reported on February 13, 2026, “Homeland Security is said to have sent Google and Meta hundreds of subpoenas for information to identify Americans who oppose ICE. Tech companies received legal requests for the names, email addresses, telephone

⁵ <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole>

⁶ <https://www.americanimmigrationcouncil.org/blog/ice-immigrationos-palantir-ai-track-immigrants/> (last visited 6/6/2026).

⁷ <https://www.nbcnews.com/tech/tech-news/facebook-turned-chat-messages-mother-daughter-now-charged-abortion-rcna42185> (last visited 6/6/2026).

⁸ <https://newrepublic.com/post/206088/homeland-security-67-year-old-us-citizen-criticized-email> (last visited 6/8/2026).

numbers and other identifying data behind social media accounts that track or criticize the agency.”⁹

46. In early March 2026, a news website reported about the existence of an U.S. Department of Homeland Security internal document revealing that Custom and Border Protection (“CPB”) “bought data from the online advertising ecosystem to track peoples’ precise movements over time ...”¹⁰

Data and Related Profiles of Consumers Have Economic Value

47. The type of visitor data transmitted via the Website to LiveRamp has economic value – as is obvious from the fact that these third parties create code to collect it, and Defendant has installed the code on the Website. The value of this data – that of Plaintiff as well as that of members of the Class on whose behalf Plaintiff has filed this action – was diminished by Defendant’s deployment of the Data Broker Code on the Website.

48. The loss of anonymity that occurs through the type of visitor browser fingerprinting and subsequent tracking alleged herein imposes real costs on visitors to Defendant’s Website, including Plaintiff and members of the putative Class in this action. For example, in 2025, the Federal Trade Commission found that many websites use data such as “consumers’ characteristics and behaviors, like location, demographics, browsing patterns and shopping history” to tailor consumer pricing.¹¹

49. As recently explained by the Law Institute:¹²

⁹ *Homeland Security Wants Social Media Sites to Expose Anti-ICE Accounts* (N.Y. Times Feb. 13, 2026), available at <https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html> (last visited 2/25/2026).

¹⁰ *CBP Tapped Into the Online Advertising Ecosystem To Track Peoples’ Movements* (404 Media Mar. 3, 2026), available at <https://www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements/> (last visited 3/16/2026); *see also Security News This Week: CBP Used Online Ad Data to Track Phone Locations* (Wired Mar. 7, 2026), available at <https://www.wired.com/story/cbp-used-online-ad-data-to-track-phone-locations/> (last visited 3/16/2026).

¹¹ *See https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer* (U.S. Federal Trade Commission Jan. 17, 2025) (last visited 2/23/2026).

¹² <https://thelaw.institute/cyberspace-technology-and-social-issues/identity-value-modern-economy/> (The Law Institute (Updated) Oct. 27, 2025) (last visited 2/23/2026).

In the modern economy, identity information has been described as the business of buying and selling information as a commodity. Unlike traditional physical commodities, personal data is intangible yet holds immense economic value. The transformation of identity into a tradeable asset has occurred gradually as technologies for collecting and analyzing personal information have become increasingly sophisticated. [. . .] Personal identity in the digital realm comprises multiple elements. Demographic information includes age, gender, location, income levels, and educational background. Behavioral data tracks online activities such as websites visited, products viewed, and time spent on particular pages. Transaction histories reveal purchasing patterns, payment methods, and brand preferences. Location data from smartphones and wearable devices provides real-time information about movements and habits. What makes identity information particularly valuable is its predictive power. By analyzing past behaviors and preferences, companies can anticipate future actions with remarkable accuracy. This ability to forecast consumer behavior translates directly into competitive advantages in marketing and product development. A complex ecosystem has emerged around the collection and trading of identity information. This marketplace operates largely invisibly to average consumers, yet it powers much of the modern digital economy. The global data brokerage industry was valued at approximately \$270.4 billion in 2024, with projections indicating growth to \$473.35 billion by 2032. [. . .] Advertisers and marketers purchase identity information to target specific consumer segments with tailored messages. Behavioral advertising uses internet cookies and tracking

technologies to understand browsing tendencies and create defined audience segments. This allows companies to place advertisements in front of consumers most likely to respond positively.

50. There exists an established market for the type of personal data collected and transmitted through the Data Broker Code running on the Website: data that facilitates the creation and enhancement of consumer profiles for individuals, and ongoing tracking of individuals' internet browsing. Defendant's surreptitious and unlawful transfer of personal information through the code on its Website diminished Plaintiff's and Class members' ability to participate in that market on informed terms, including to exercise the choice of whether to withhold, limit, or exchange their personal data for value.

CLASS ALLEGATIONS

51. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class") defined as follows:

All persons who, while located in California, visited the Website during the applicable limitations period, and were subjected to the operation of the Data Broker Code running on the Website.

52. This action has been brought and may be properly maintained as a class action. There is a well-defined community of interest in the litigation and the proposed class is ascertainable.

53. 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 may be ascertained by the records maintained by Defendant.

54. 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:

- a. Whether Defendant's actions violate California common or statutory law;

- b. Whether Plaintiff and Class members are entitled to statutory damages;
- c. Whether Plaintiff and Class members are entitled to punitive damages;
- d. Whether Plaintiff and Class members are entitled to injunctive relief;
- e. Whether Plaintiff and Class members are entitled to the disgorgement of unlawfully obtained data; and
- f. Whether Plaintiff and Class members are entitled to the disgorgement of profits.

55. TYPICALITY: Plaintiff was subjected to the Data Broker Code running on the Website when she visited the Website on October 5, 2025. As a result, her data was transmitted to LiveRamp, and possibly other third parties, for fingerprinting/identification and tracking purposes. Her claims are therefore typical of the Class.

56. 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.

57. SUPERIORITY: A class action is superior to other available methods of adjudication because individual litigation of the claims of each Class member 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 and address identical issues.

FIRST CAUSE OF ACTION

Violations of California Trap and Trace Law, Cal. Penal Code § 638.51

58. Plaintiff and Class Members reallege and incorporate each allegation in all preceding paragraphs contained herein.

59. The California Trap and Trace Law provides that “a person may not install or use...a trap and trace device without first obtaining a court order....” Cal. Penal Code § 638.51(a).

60. A “trap and trace device” is defined as “a device or process that captures the 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, but not the contents of a communication.” § 638.50(c).

61. The Data Broker Code, as deployed on the Website, constitutes a trap and trace device under Cal. Penal Code § 638.50(c).

62. The “electronic communication” at issue in this case is the communication between the devices of Plaintiff and the Class members, on the one hand, and the Website, an instrumentality of Defendant, on the other hand. “Electronic communication” is defined under CIPA as “any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.” A visit to a website entails the transfer of signals and data, or “intelligence of any nature” by a “wire, radio [or] electromagnetic [. . .] system.” Cal. Penal Code § 629.51(a)(2). The interactions of Plaintiff and Class members with the Website meet this definition.

63. The Data Broker Code is designed to identify the source of the electronic communications between the devices of Plaintiff and Class members, on the one hand, and the Website, on the other, by “captur[ing]” the electronic or other impulses emanating from the devices that are “incoming” to the Website. The “*sources*” of the electronic communications moving from the devices to the Website are ***Plaintiff and the Class members (including their devices)***.

64. Software or code running on websites that “captures the 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” constitutes a trap and trace device for purposes of §§ 638.50-51. *See, e.g., Biglang-Awa-Castro v. SBE Restaurant Group, LLC*, 25VECV03590, 2026 Cal. Super. LEXIS 29752, at *3-4 (L.A. Co. Super. Ct. Apr. 16, 2026); *Schallert v. RocketGenius*, 25STCV35081, 2026 Cal. Super. LEXIS 25177, at *3-4 (L.A. Co. Super. Ct. March 24, 2026); *Hassid v. Alex & Ani, LLC*, 2026 U.S. Dist. LEXIS 11238, at *4-7 (C.D. Cal. Jan. 20, 2026); *Casillas v. Lucky Opco LLC*, 25STCV03961, 2026 Cal. Super. LEXIS 24132, at *5-6 (L.A. Co. Super. Ct. Jan. 5, 2026); *Casillas v. Six Flags Ent. Corp.*, 812 F. Supp. 3d 1016, 1030-32 (C.D. Cal. 2025); *Lewis v. Magnite, Inc.*, 2025 U.S. Dist. LEXIS 263675, at *39-42 (C.D. Cal. Dec. 4, 2025); *Santoro v. Lulu*

& Georgia, Inc., 25STCV11722, 2025 Cal. Super. LEXIS 84529, at *8-9 (L.A. Co. Super. Ct. Nov. 21, 2025); *Zhizhi Xu v. Reuters News & Media, Inc.*, 25CV459918, 2025 Cal. Super. LEXIS 76169, at *8-10 (Santa Clara Co. Super Ct. Oct. 24, 2025); *Scarlett v. Future US, LLC*, CGC-25-621912, 2025 Cal. Super. LEXIS 56166, at *11-14 (S.F. Co. Super. Ct. Sept. 5, 2025); *Garon v. Keleops USA, Inc.*, 2025 U.S. Dist. LEXIS 170745, at *10-15 (N.D. Cal. Sep. 2, 2025); *Valenzuela v. Intersystems Corp.*, 2025 Cal. Super. LEXIS 42550, at *3-4 (Orange Co. Superior Ct. Aug. 4, 2025); *Riganian v. The Data Brokers Holdings, Inc.*, 791 F.Supp.3d 1075, 1093-1094 (N.D. Cal. July 18, 2025); *Gabrielli v. Motorola Mobility LLC*, 2025 U.S. Dist. LEXIS 133836, at *30-32 (N.D. Cal. July 14, 2025); *Price v. Headspace, Inc.*, 2025 Cal. Super. LEXIS 27951, at *3-9 (L.A. Super Ct. Apr. 1, 2025); *Sanchez v. Glasscanopy, Inc.*, 2025 Cal. Super. LEXIS 18460, at *8-9 (L.A. Super. Ct. Feb. 28, 2025); *Heiting v. Fka Distrib. Co.*, 2025 U.S. Dist. LEXIS 20076, at *8 (C.D. Cal. Feb. 3, 2025); *Conohan v. Rad Power Bikes Inc.*, 2025 U.S. Dist. LEXIS 72865, 2025 WL 1111246, at *16 (C.D. Cal. Apr. 3, 2025); *Mirmalek v. Los Angeles Times Commc'ns LLC*, 2024 U.S. Dist. LEXIS 227378, at *6-10 (N.D. Cal. Dec. 12, 2024); *Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 930-931 (N.D. Cal. October 21, 2024); *Moody v. C2 Educ. Sys. Inc.*, 742 F. Supp. 3d 1072, 1076-1077 (C.D. Cal. July 25, 2024).

65. Defendant did not obtain a court order before using or installing the Data Broker Code on the Website. Defendant also did not obtain consent from Plaintiff or any of the Class Members before using this technology, which is designed to identify Plaintiff and the Class members, along with their devices, as the source of electronic communications between them, on the one hand, and the Website, an instrumentality of Defendant, on the other hand.

66. Defendant did not obtain the express or implied consent of Plaintiff or Class members to be subjected to data-sharing or data-selling with or by or through LiveRamp.

67. Defendant is ineligible for the statutory consent exemption from liability for use of a trap and trace device set forth in Cal. Penal Code § 638.51(b)(5). The § 638.51(b)(5) consent exemption is available only to a “provider of electronic or wire communication service.” Defendant is not such a provider.

68. Defendant's conduct violating § 638.51 caused Plaintiff and the Class members significant injuries. These injuries include: invasion of their legally protected privacy rights; their loss of control over personal identifying information due to Defendant's actions; the diminution in value of their data and identity; Defendant's unauthorized creation of detailed behavioral profiles of them; their mental anguish from knowledge of Defendant's secret monitoring; and chilling effects on their free online expression and inquiry due to Defendant's conduct, including causing the ongoing monitoring of their internet activity.

69. CIPA imposes civil liability including statutory damages for violations of the California Trap and Trace Law. Cal. Penal Code § 637.2; *see also Fandom*, 754 F. Supp. 3d at 932; *C2 Educ. Sys. Inc.*, 742 F. Supp. 3d at 1077-78.

70. Plaintiff and Class members are entitled to statutory damages of \$5,000 for each of Defendant's violations of § 638.51.

SECOND CAUSE OF ACTION

Intrusion Upon Seclusion

71. Plaintiff and Class Members reallege and incorporate each allegation in all preceding paragraphs contained herein.

72. Under California law, a defendant is liable for intrusion upon seclusion when it intentionally intrudes into a private place, conversation, or matter in a manner that would be highly offensive to a reasonable person.

73. Defendant's deployment of the Data Broker Code on the Website intentionally intruded into a private conversation or matter Plaintiff and the Class members were involved in – namely their visit to the Website. The intrusion allowed LiveRamp to identify, profile and track (on an ongoing basis) Plaintiff and Class members.

74. Plaintiff and the Class members never authorized the third-party cookies and other tracking technology initiated by the Data Broker Code on the Website.

75. Plaintiff and Class members had an objectively reasonable expectation of privacy with respect to their conversation or exchange with Defendant over the Website.

76. Defendant's intrusion into Plaintiff's and Class members' visits to the Website was intentional, in that it involved deployment of software and configuration of the Website. Further, it was perpetrated for Defendant's economic benefit.

77. Deployment of tracking software that engages in the type of identification, profiling and tracking carried out by the Data Broker Code that Defendant installed on the Website forms the basis of an actionable intrusion upon seclusion claim under California law. *See, e.g., Caldwell v. InMobi Pte., Ltd.*, No. 25-cv-09977-AMO, 2026 U.S. Dist. LEXIS 94801, at *7-14 (N.D. Cal. Apr. 29, 2026); *Casillas v. Six Flags Ent. Corp.*, 812 F. Supp. 3d 1016, 1029-30 (C.D. Cal. 2025); *Krzyzek v. Openx Techs., Inc.*, No. 25-cv-05588-SI, 2026 U.S. Dist. LEXIS 15195, at *10-13 (N.D. Cal. Jan. 27, 2026).

78. The intrusion described herein would be highly offensive to a reasonable person.

79. Defendant's intrusion upon seclusion caused Plaintiff and the Class members significant injuries. These injuries include: Defendant's invasion of their legally protected privacy rights; their loss of control over personal identifying information due to Defendant's actions; the diminution in value of their data and identity; Defendant's unauthorized creation of detailed behavioral profiles of them; their mental anguish from knowledge of Defendant's secret monitoring; and chilling effects on their free online expression and inquiry due to Defendant's conduct, including causing the ongoing monitoring of their internet activity.

80. Defendant's invasion of the privacy of Plaintiff and Class members damaged them and they are there entitled to compensatory damages, which includes monetary damages.

81. Plaintiff and Class members are entitled additionally to punitive damages because Defendant's use of the Data Broker Code on the Website was malicious, oppressive and willful.

82. Plaintiff and Class members are entitled additionally to equitable relief in the form of enjoining Defendant from continuing to engage in its unlawful conduct, and disgorgement of profits earned by Defendant from its invasion of their privacy interests.

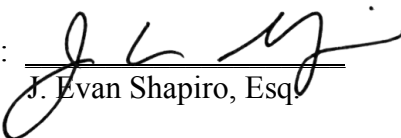
PRAYER

WHEREFORE, Plaintiff, on her behalf and on behalf of the Class members, prays for the following relief against Defendant:

1. An order certifying the Class, naming Plaintiff as the representative of the Class and appointing Plaintiff's attorneys as Class Counsel;
2. An award of statutory damages pursuant to CIPA;
3. An award of punitive damages;
4. An award of nominal damages;
5. An order for full restitution;
6. An order requiring Defendant to disgorge revenues and profits wrongfully obtained;
7. An order enjoining Defendant's conduct as alleged herein and any other injunctive relief that the Court finds proper;
8. Reasonable attorneys' fees and costs; and
9. All other relief that would be just and proper as a matter of law or equity, as determined by the Court.

DATED: July 28, 2026

TAULER SMITH LLP

By: 

J. Evan Shapiro, Esq.

J. Evan Shapiro
Robert Tauler
90 Broad St., Suite 703
New York, New York 10004
eshapiro@taulersmith.com
rtauler@taulersmith.com
(212) 702-8670 (New York office)
(213) 927-9270 (Main Office (L.A.))

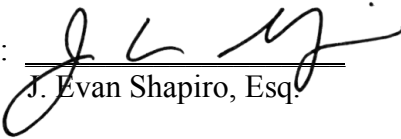
Attorneys for Plaintiff Carol Price

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury.

DATED: July 28, 2026

TAULER SMITH LLP

By: 
J. Evan Shapiro, Esq.

J. Evan Shapiro
Robert Tauler
90 Broad St., Suite 703
New York, New York 10004
eshapiro@taulersmith.com
rtauler@taulersmith.com
(212) 702-8670 (New York office)
(213) 927-9270 (Main Office (L.A.))

Attorneys for Plaintiff Carol Price