Exhibit A

BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Emily A. Horne (State Bar No. 347723)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
          ehorne@bursor.com

Attorneys for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ALAMEDA

TALIAH MIRMALEK, individually and on behalf of all others similarly situated,
 	
                    Plaintiff,
 	
     v.
 	
LOS ANGELES TIMES COMMUNICATIONS LLC,
 	
                    Defendant.
	Case No.
	
	CLASS ACTION COMPLAINT
	
	<u>JURY TRIAL DEMANDED</u>

Plaintiff Taliah Mirmalek ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself and her counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. Defendant Los Angeles Times Communications LLC ("Defendant") owns and operates a website, LATimes.com (the "Website" or "LA Times").

2. When users visit the Website, Defendant causes three trackers—the TripleLift Tracker, GumGum Tracker, and Audiencerate Tracker (collectively, the "Trackers")—to be installed on Website visitors' internet browsers. Defendant then uses these Trackers to collect Website visitors' IP addresses.

3. Because the Trackers capture Website visitors' "routing, addressing, or signaling information," the Trackers each constitute a "pen register" under Section 638.50(b) of the California Invasion of Privacy Act ("CIPA"). Cal. Penal Code § 638.50(b); s*ee also Greenley v. Kochava, Inc.*, 2023 WL 4833466 (S.D. Cal. July 27, 2023).

4. By installing and using the Trackers without Plaintiff's prior consent and without a court order, Defendant violated CIPA § 638.51(a).

5. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents, and to recover statutory damages for Defendant's violation of CIPA § 638.51.

PARTIES

6. Plaintiff Mirmalek resides in Oakland, California and has an intent to remain there, and is therefore a citizen of California. Plaintiff Mirmalek was in California when she visited the Website.

7. Defendant Los Angeles Times Communications LLC is a Delaware Limited Liability Company, with its principal place of business located in California.

JURISDICTION AND VENUE

8.   This Court has subject matter jurisdiction over this action pursuant to Article VI, Section 10 of the California Constitution and Cal. Code Civ. Proc. § 410.10. This action is brought as a class action on behalf of Plaintiff and Class Members pursuant to Cal. Code Civ. Proc. § 382.

9.   This Court has personal jurisdiction over Defendant because it is headquartered and conducts business in this State.

10.   Venue is proper in this District because the conduct alleged in this Complaint occurred in this County.

FACTUAL ALLEGATIONS

I.   THE CALIFORNIA INVASION OF PRIVACY ACT

11.   The California Legislature enacted CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

12.   As relevant here, CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

13.   A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

14.   A "trap and trace device" is a "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." Cal. Penal Code § 638.50(b).

15.   In plain English, a "pen register" is a "device or process" that records *outgoing* information, while a "trap and trace device" is a "device or process" that records *incoming* information.

---

16.   Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology advanced, however, courts have expanded the application of these surveillance devices.

17.   For example, if a user sends an email, a "pen register" might record the email address it was sent from, the email address the email was sent to, and the subject line—because this is the user's *outgoing* information. On the other hand, if that same user receives an email, a "trap and trace device" might record the email address it was sent from, the email address it was sent to, and the subject line—because this is *incoming* information that is being sent to that same user.

18.   Although CIPA was enacted before the dawn of the Internet, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013); *see also Greenley*, 2023 WL 4833466, at *15 (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v. Assurance IQ*, LLC, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications."). This accords with the fact that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

19.   Individuals may bring an action against the violator of any provision of CIPA—including CIPA § 638.51—for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

II.   DEFENDANT VIOLATES THE CALIFORNIA INVASION OF PRIVACY ACT

A.   The Trackers Are "Pen Registers"

20.   To make Defendant's Website load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to Defendant's server where the relevant Website data is stored. In response to the request, Defendant's server sends an "HTTP response" back to the browser with a set of instructions. *See* Figure 1.

21.   The server's instructions include how to properly display the Website—*e.g.*, what images to load, what text should appear, or what music should play.

22.   In addition, the server's instructions cause the Trackers to be installed on a user's browser. The Trackers then cause the browser to send identifying information—including the user's IP address—to TripleLift, GumGum, and Audiencerate.

23.   The IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). The first two sets of numbers indicate what network the device is on (*e.g.*, 192.168), and the second two sets of numbers identify the specific device (*e.g.*, 123.132). Thus, the IP address enables a device to communicate with another device— such as a computer's browser communicating with a server—and the IP address contains geographical location. Through an IP address, the device's state, city, and zip code can be determined.

24.   As alleged below, Defendant installs each of the Trackers on the user's browser, and the Trackers collect information—users' IP addresses—that identifies the outgoing "routing, addressing, or signaling information" of the user. Accordingly, the Trackers are each "pen registers."

1.   *TripleLift Tracker*

25.   TripleLift is a software-as-a-service company that develops the TripleLift Tracker, which it provides to website owners, like Defendant, for a fee.

26.   According to TripleLift, its "technology powers ads that make advertising better for everyone—higher performing for brands, more lucrative for publishers and more respectful of the

consumer's experience."[1]

27. In other words, TripleLift enables companies to sell advertising space on their website, thereby earning revenue, and allows companies to place advertisements on other companies' websites, thereby driving brand awareness and sales. To achieve this, TripleLift uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

28. The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the TripleLift Tracker on the user's browser. The TripleLift Tracker, in turn, instructs the user's browser to send TripleLift the user's IP address.

29. Moreover, TripleLift stores a cookie with the user's IP address in the user's browser cache. When the user subsequently visits Defendant's Website, the TripleLift Tracker instructs the user's browser to send the user's IP address through the cookie. *See* Figure 2.

Figure 2:

30. If the user clears his or her cookies, then the user wipes out the TripleLift Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the TripleLift Tracker on the user's browser, (ii) the TripleLift Tracker instructs the browser to send TripleLift the user's IP address, (iii) the TripleLift Tracker stores a cookie in the browser cache, and (iv) TripleLift will continue to receive the user's IP address on subsequent Website visits through the cookie.

_____

[1] *Technology*, TRIPLELIFT, https://triplelift.com/technology (last visited Jan. 9, 2024).

31.   In all cases, however, TripleLift receives a user's IP address each and every time a user interacts with the website of one of TripleLift's clients, including Defendant's Website. Indeed, the IP address is transmitted to TripleLift along with the cookie value, as the below screenshot indicates. *See* Figure 3.

Figure 3:

32.   The TripleLift Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 2023 WL 4833466, at *15.

33.   Further, the TripleLift Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James v. Walt Disney Co.*, --- F. Supp. 3d ---,

2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023).

34.   Because the TripleLift Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA§ 638.50(b).

   2.   GumGum Tracker

35.   GumGum, Inc. ("GumGum") is a software-as-a-service company that develops the GumGum Tracker, which it provides to website owners like Defendant for a fee.

36.   According to GumGum, it "delivers the next generation of contextual intelligence, industry leading ad creatives, and the ability to measure and optimize advertising campaigns to better understand a consumer's mindset that captures attention and drives action and outcomes."[2]

37.   In other words, GumGum enables companies to sell advertising space on their websites, thereby earning revenue, and allows companies to place advertisements on other companies' websites, thereby driving brand awareness and sales. To achieve this, GumGum uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

38.   The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the GumGum Tracker on the user's browser. The GumGum Tracker, in turn, instructs the user's browser to send GumGum the user's IP address.

39.   Moreover, GumGum stores a cookie with the user's IP address in the user's browser cache. When the user subsequently visits Defendant's Website, the GumGum Tracker instructs the user's browser to send the user's IP address through the cookie. *See* Figure 2, *supra*.

40.   If the user clears his or her cookies, then the user wipes out the GumGum Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the GumGum Tracker on the user's browser, (ii) the GumGum Tracker instructs the browser to send GumGum the user's IP address, (iii) the GumGum Tracker stores a cookie in the browser cache, and (iv) GumGum will continue to receive the user's IP address on subsequent Website visits through the cookie.

---

[2] *About*, GUMGUM, https://gumgum.com/about (last visited Jan. 4, 2024).

41.   In all cases, however, GumGum receives a user's IP address each and every time a user interacts with the website of one of GumGum's clients, including Defendant's Website. Indeed, the IP address is transmitted to GumGum along with the cookie value, as the below screenshot indicates. *See* Figure 4.

<u>Figure 4:</u>

42.   The GumGum Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 2023 WL 4833466, at *15.

43.   Further, the GumGum Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James v. Walt Disney Co.*, --- F. Supp. 3d ---, 2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023).

44.   Because the GumGum Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA § 638.50(b).

3.   *Audiencerate Tracker*

45.   Audiencerate LTD ("Audiencerate") is a software-as-a-service company that develops the Audiencerate Tracker, which it provides to website owners like Defendant for a fee.

46.   According to Audiencerate, it "enable[s] data-driven advertising via [its] proprietary technology and platforms."[3]

47.   "One side of [Audiencerate's] business is dedicated to helping data owners monetize their data and license audiences in the world's largest programmatic media buying marketplaces. The other side provides targeting data to marketers, enabling them to model and target audiences with more complexity and sophistication."[4]

48.   Just like TripleLift and GumGum, Audiencerate uses its Tracker to receive, store, and analyze data collected from website visitors, including visitors of Defendant's Website.

49.   The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends the HTTP response. This response also includes directions to install the Audiencerate Tracker on the user's browser. The Audiencerate Tracker, in turn, instructs the user's browser to send the user's IP address to Audiencerate.

50.   Moreover, Audiencerate stores a cookie with the user's IP address in the user's browser cache. When the user subsequently visits Defendant's Website, the Audiencerate Tracker instructs the user's browser to send the user's IP address through the cookie. *See* Figure 2, *supra*.

51.   If the user clears his or her cookies, then the user wipes out the Audiencerate Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the Audiencerate Tracker on the user's browser, (ii) the Audiencerate Tracker instructs the browser to send Audiencerate the user's IP address, (iii) the Audiencerate Tracker stores a cookie in the browser cache, and (iv) Audiencerate will continue to

---

[3] AUDIENCERATE, https://www.audiencerate.com/ (last visited Jan. 4, 2024).
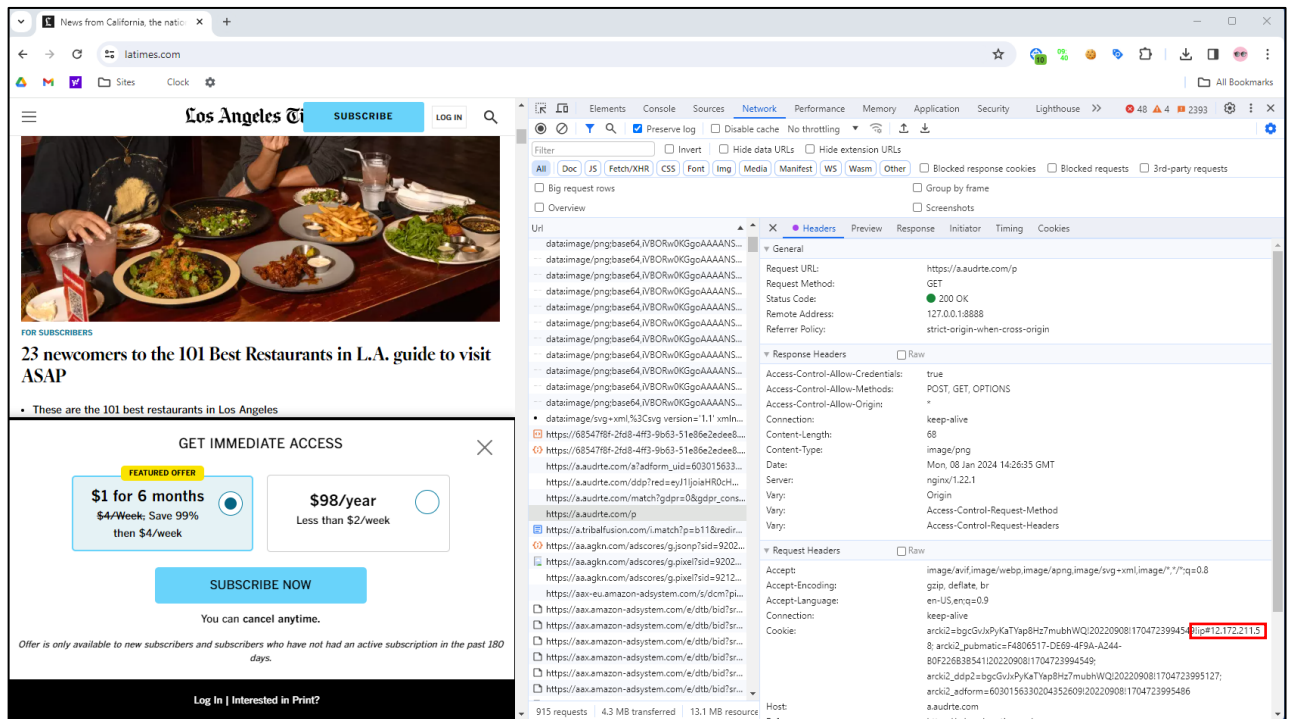
[4] *AWS Enables Audiencerate to Process Over a Billion Requests per Week*, AWS (2020), https://aws.amazon.com/solutions/case-studies/audiencerate-case-study/.

receive the user's IP address on subsequent Website visits through the cookie.

52. In all cases, however, Audiencerate receives a user's IP address each and every time a user interacts with the website of one of Audiencerate clients, including Defendant's Website.

53. Indeed, the IP address is transmitted to Audiencerate along with the cookie value. *See* Figure 5.

Figure 5:

54. The Audiencerate Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 2023 WL 4833466, at *15.

55. Further, the Audiencerate Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James*, 2023 WL 7392285, at *13.

56. Because the Audiencerate Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA§ 638.50(b).

B. Defendant Installed And Used The Trackers On Plaintiff's And Class Members' Browsers Without Prior Consent Or A Court Order

57. Defendant owns and operates the Website, which boasts "more than 40 million unique

… visitor[s] monthly."[5]

58.   The Website provides local, state, national, and international news, as well as online games, short documentaries, op-eds, entertainment and arts information, obituaries, and recipes.

59.   When companies build their websites, they install or integrate various third-party scripts into the code of the website in order to collect data from users or perform other functions.[6]

60.   Often times, third-party scripts are installed on websites "for advertising purposes."[7]

61.   Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time."[8]

62.   Since at least February 2023, if not earlier, Defendant has incorporated the code of the Trackers into the code of its Website. Thus, when Plaintiff visited the Website, the Website caused the Trackers to be installed on Plaintiff's and other users' browsers.

63.   As outlined above, when a user visits the Website, the Website's code—as programmed by Defendant—installs the Trackers onto the user's browser.

64.   Upon installing the Trackers on its Website, Defendant uses the Trackers to collect the IP address of visitors to the Website, including the IP address of Plaintiff and Class Members. *See* Figures 6 (TripleLift Tracker), 7 (GumGum Tracker), and 8 (Audiencerate Tracker).

---

[5] *About The Los Angeles Times*, LOS ANGELES TIMES, https://www.latimes.com/about (last visited Jan. 4, 2024).
[6] *See* THIRD-PARTY TRACKING, https://piwik.pro/glossary/third-party-tracking/ ("Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user's visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user's browsing history to other companies…").
[7] *Id.*
[8] *Id.*

Figure 6:

4661	18.488488517	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	283 Application Data
6528	18.842908824	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	206 Application Data
11266	23.201098758	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	157 Application Data
11329	23.263487966	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	187 Application Data
11330	23.263536990	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	286 Application Data
11424	23.312333633	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	202 Application Data
11425	23.312365723	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	191 Application Data
11426	23.312387671	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	182 Application Data
11427	23.312410334	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	218 Application Data
11428	23.312433809	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	173 Application Data
11507	23.357376510	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	139 Application Data
11690	23.464840074	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	191 Application Data
11716	23.499390150	192.168.200.39	us-east-eb2.3lift.com	TLSv1.3	101 Application Data
3309	17.833670630	192.168.200.39	us-east-tlx.3lift.com	TLSv1.3	815 Client Hello
3382	17.864442946	192.168.200.39	us-east-tlx.3lift.com	TLSv1.3	130 Change Cipher Spec, Applica
3383	17.864547344	192.168.200.39	us-east-tlx.3lift.com	TLSv1.3	158 Application Data
3384	17.864654078	192.168.200.39	us-east-tlx.3lift.com	TLSv1.3	523 Application Data
3385	17.864684966	192.168.200.39	us-east-tlx.3lift.com	TLSv1.3	2937 Application Data
3478	17.894159218	192.168.200.39	us-east-tlx.3lift.com	TLSv1.3	97 Application Data
13633	34.023469938	192.168.200.39	us-east-tlx.3lift.com	TLSv1.3	223 Application Data

Figure 7:

No.	Time	Source	Destination	Protocol	Length	Info
14132	34.954173599	192.168.200.39	user-data-us-east.bidswi…	TLSv1.2	159	Client Key Exchange, Change
14133	34.954545145	192.168.200.39	user-data-us-east.bidswi…	TLSv1.2	931	Application Data
14189	35.108152742	192.168.200.39	user-data-us-east.bidswi…	TLSv1.2	924	Application Data
14768	36.514824930	192.168.200.39	user-data-us-east.bidswi…	TLSv1.2	941	Application Data
15187	36.823755886	192.168.200.39	user-data-us-east.bidswi…	TLSv1.2	969	Application Data
5911	18.702414451	192.168.200.39	usersync.gumgum.com	TLSv1.3	669	Client Hello
5915	18.704340589	192.168.200.39	usersync.gumgum.com	TLSv1.3	637	Client Hello
5985	18.722228712	192.168.200.39	usersync.gumgum.com	TLSv1.3	669	Client Hello
6021	18.726297271	192.168.200.39	usersync.gumgum.com	TLSv1.3	669	Client Hello
6026	18.727289119	192.168.200.39	usersync.gumgum.com	TLSv1.3	637	Client Hello
6033	18.728473990	192.168.200.39	usersync.gumgum.com	TLSv1.3	583	Client Hello
6066	18.733110506	192.168.200.39	usersync.gumgum.com	TLSv1.3	130	Change Cipher Spec, Applica

Figure 8:

3121	17.763540442	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	875 Client Hello
3187	17.791767532	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	130 Change Cipher Spec, Applica
3188	17.791828614	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	158 Application Data
3190	17.791895846	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	428 Application Data
3206	17.799149806	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	97 Application Data
3243	17.808236052	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	105 Application Data
3659	17.953286945	192.168.200.39	95.158.160.34.bc.googleu…	QUIC	1292 Initial, DCID=a372dfa7e26f7
3663	17.954773594	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	193 Application Data
3674	17.961028023	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	101 Application Data
3675	17.961053819	192.168.200.39	95.158.160.34.bc.googleu…	TLSv1.3	105 Application Data
7388	19.057791436	192.168.200.39	a-us-east.rfihub.com.aka…	TLSv1.3	630 Client Hello
7629	19.101742772	192.168.200.39	a-us-east.rfihub.com.aka…	TLSv1.3	130 Change Cipher Spec, Applica
7646	19.104868031	192.168.200.39	a-us-east.rfihub.com.aka…	TLSv1.3	695 Application Data
11921	24.371966544	192.168.200.39	a-us-east.rfihub.com.aka…	TLSv1.3	1142 Application Data
15168	36.753502647	192.168.200.39	a-us00.kxcdn.com	TLSv1.3	630 Client Hello
15215	37.019377981	192.168.200.39	a-us00.kxcdn.com	TLSv1.3	146 Change Cipher Spec, Applica
15216	37.019651145	192.168.200.39	a-us00.kxcdn.com	TLSv1.3	158 Application Data
15217	37.019862575	192.168.200.39	a-us00.kxcdn.com	TLSv1.3	458 Application Data
15306	37.766348341	192.168.200.39	a-us00.kxcdn.com	TLSv1.3	97 Application Data
12759	27.490744714	192.168.200.39	a.audrte.com	TLSv1.2	662 Client Hello
12790	27.627332130	192.168.200.39	a.audrte.com	TLSv1.2	192 Client Key Exchange, Change
12824	27.761896714	192.168.200.39	a.audrte.com	TLSv1.2	736 Application Data

65.   Defendant then uses the IP address of Website visitors, including those of Plaintiff and Class Members, to serve targeted advertisements and conduct website analytics.

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

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

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

68.   As alleged herein, the Trackers are designed to analyze Website data and marketing campaigns, conduct targeted advertising, and boost Defendant's revenue, all through their surreptitious collection of Plaintiff's and Class Members' data.

1.   Defendant Discloses User's Data To TripleLift For The Purpose Of Marketing, Advertising, And Analytics

69.   TripleLift describes itself as a digital advertising platform that "work[s] for everyone: publishers who seek greater monetization, advertisers who require better performance, [and] consumers who want better ad experiences."[9]

70.   TripleLift helps companies like Defendant market, advertise, and analyze user data from its website. For example, TripleLift enables publishers to place advertisements on their webpages, in videos, or embedded in broadcasts. To ensure that an effective advertisement is shown to the consumer, the publisher shares data about the user with TripleLift and TripleLift serves the targeted ad.[10]

71.   TripleLift also helps advertisers select where to place their ads through "TripleLift Audiences," which "span[s] third-party and first-party data."[11] In other words, TripleLift utilizes

---

[9] *Who We Are*, TRIPLELIFT, https://triplelift.com/company (last visited Jan. 9, 2024).

[10] *See Smart Data & Targeting For Publishers*, TRIPLELIFT, https://triplelift.com/products/audiences-publishers (last visited Jan. 9, 2024).

[11] *Smart Data & Targeting For Advertisers*, TRIPLELIFT, https://triplelift.com/products/audiences-advertisers (last visited Jan. 9, 2024).

third-party data, as well as data from the publisher where the ad is ultimately placed (*i.e.*, first-party), to determine where to place advertisers' ads and who to place them in front of.

72.   By way of example, if a home-goods brand wants to use TripleLift to serve its ads, it can purchase TripleLift's "Home Curated Deal" to reach "people who are investing their time and money close to home."[12] By choosing this set of data, the home-goods brand will be able to target "audiences spending time on home improvement, home entertaining, outfitting their setups, browsing real estate, raising kids and adopting pets."[13] This data set can be used for ads in the "Native, Display and Video" formats, "in placements known to deliver high viewability and high video completion rates."[14] TripleLift ensures that the data sets "are refreshed on an on-going basis so that only the highest performing placements are included."[15]

73.   In other words, when users visit Defendant's Website, Defendant utilizes the TripleLift Tracker to collect IP addresses so that Defendant can analyze user data, create and analyze the performance of marketing campaigns, and target specific users or specific groups of users for advertisements. All of this helps Defendant further monetize its Website and maximize revenue by collecting and disclosing user information.

> 2.   *Defendant Discloses User's Data To GumGum For The Purpose Of Marketing, Advertising, And Analytics*

74.   GumGum is a digital advertising platform that prides itself on its "ability to measure and optimize advertising campaigns to better understand a consumer's mindset that captures attention and drives action and outcomes."[16]

75.   GumGum helps companies like Defendant market, advertise, and analyze user data from its website. One way GumGum assists with marketing and advertising is through its Ad Exchange, which is a direct marketplace where publishers and advertisers can buy and sell digital

---

[12] *HOME*, TRIPLELIFT, https://triplelift.com/exchange-traded-deals/home (last visited Jan. 9, 2024).
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *About*, GUMGUM, https://gumgum.com/about (last visited Jan. 3, 2024).

---

advertising space.[17]   Thus, when a user enters a website, GumGum enables companies to instantaneously buy and sell ad space in a way that it optimized to the particular user.

76.   According to GumGum, it uses artificial intelligence to scan the information on a web page to "deliver ads that are always relevant and align with what users are watching, reading and browsing online."[18] GumGum boasts that their "solution offers higher quality ads and increased scale across thousands of premium publisher sites" and "allow[s] advertisers to maximize their KPIs by targeting audience through customized segments such as multicultural and sustainability."[19]

77.   GumGum also offers companies "Attention Metrics," which analyzes "the amount of time and focus an individual gives to a particular advertisement or piece of content."[20] This allows companies to "[t]arget consumers where they are most attentive, ensuring maximum performance and ad relevance for [its] brand."[21] Thus, GumGum "helps advertisers optimize ad delivery to places where consumer attention is highest … [and] presents a wealth of opportunities to optimize campaign results [and] amplify brand lift."[22]

78.   In order to perform the functions listed above, GumGum needs to collect data that identifies a particular user. This is why GumGum collects IP addresses: it allows GumGum to ascertain a user's location and target that user with advertisements tailored to their location, as well as to track a user's Website activity over time (*i.e.*, through repeated Website visits) to target a user with advertisements relevant to the user's personal browsing activity.

79.   Notably, GumGum claims that it uses "cookieless targeting" to drive significant brand KPIs, thereby not collecting personal identifiable information.[23] However, GumGum is setting a visitor cookie for the user session, which transmits a user's IP addresses and other pieces of

---

[17] *Exchange*, GUMGUM, https://gumgum.com/exchange (last visited Jan. 3, 2024).

[18] *Contextual vs. Behavioral Targeting*, GUMGUM (Dec. 29, 2022), https://gumgum.com/blog/contextual-vs-behavioral-targeting.

[19] *GumGum Annoucnes Industry's First 100% Brand Safe Ad Exchange*, GUMGUM (March 15, 2023), https://gumgum.com/press-releases/brand-safe-exchange.

[20] *Attention*, GUMGUM, https://gumgum.com/attention (last visited Jan. 3, 2024).

[21] *Id.*

[22] *Id.*

[23] *Verity*, GUMGUM, https://gumgum.com/verity (last visited Jan. 3, 2024).

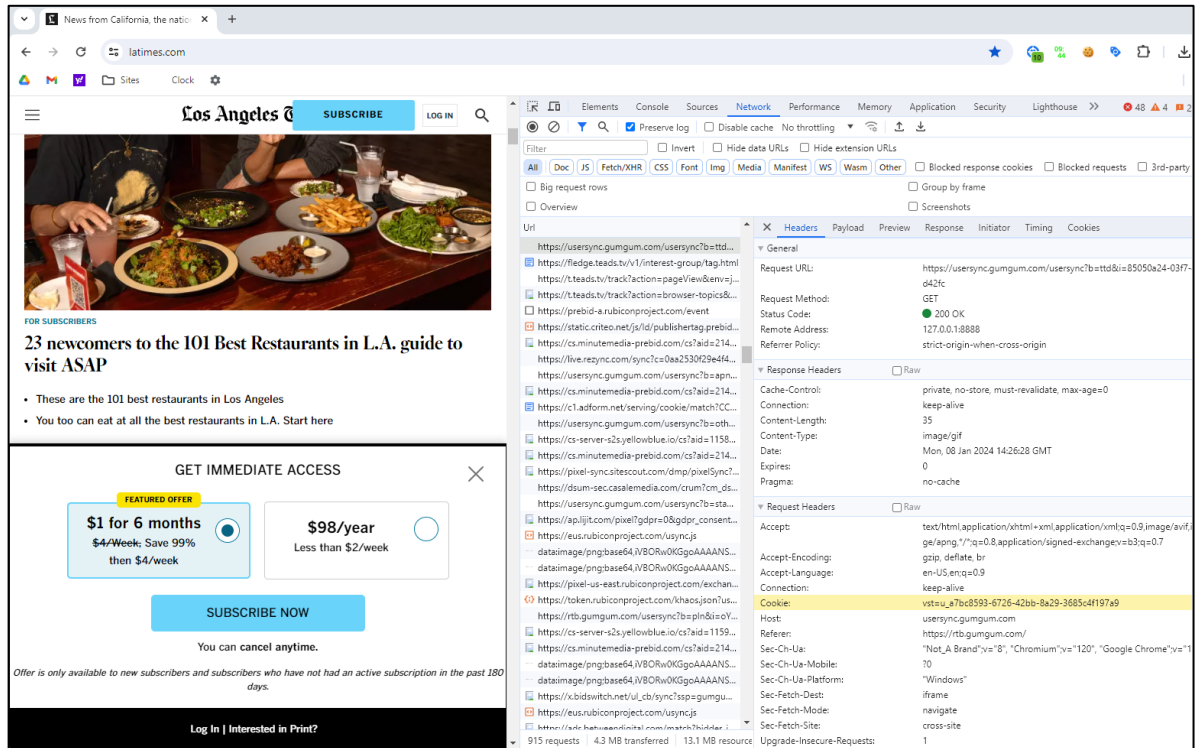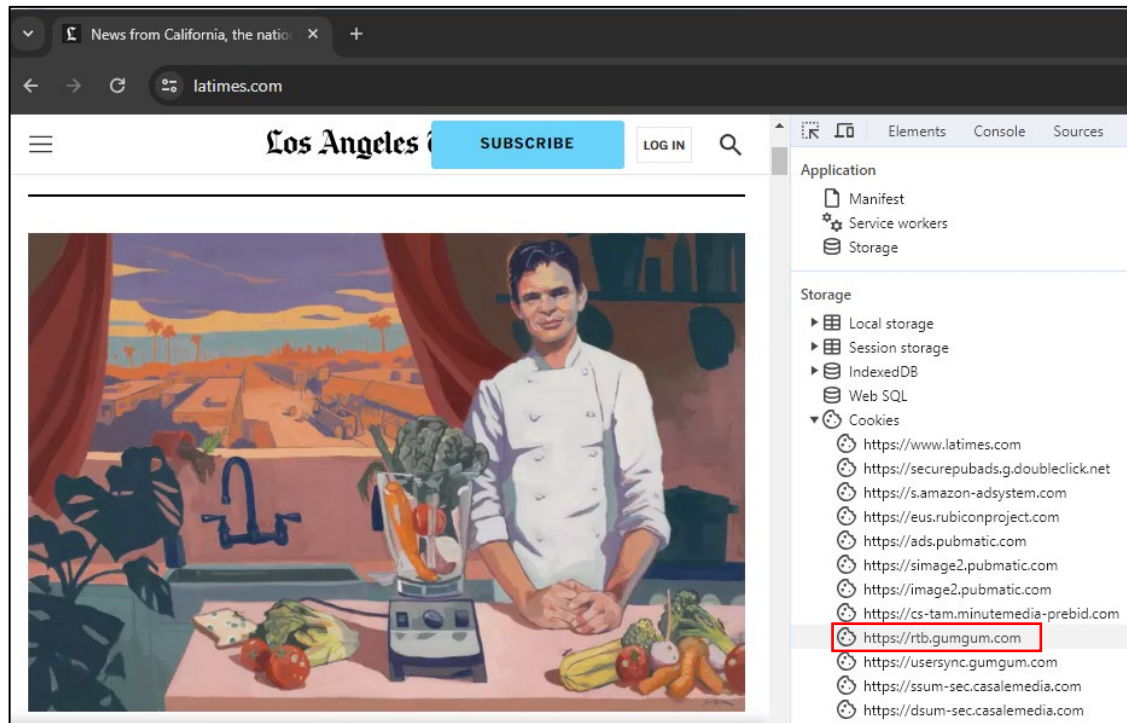information. *See* Figure 9.

Figure 9:

80.   Indeed, GumGum is actually listed as a cookie when using browser developer tools to examine the Website. *See* Figure 10.

Figure 10:

81. In other words, when users visit Defendant's Website, Defendant utilizes the GumGum Tracker to collect IP addresses so that Defendant can analyze user data, create and analyze the performance of marketing campaigns, and target specific users or specific groups of users for advertisements. All of this helps Defendant further monetize its Website and maximize revenue by collecting and disclosing user information.

            3.   *Defendant Discloses User's Data To Audiencerate For The Purpose Of Marketing, Advertising, And Analytics*

82. Whereas GumGum specifically enables advertisements on websites, Audiencerate is a data platform that "enable[s] data-driven advertising via [its] proprietary technology and platforms" for marketing, advertising, and analysis purposes.[24]

83. Companies such as Defendant share their users' data with Audiencerate through "daily synchronization" via the Audiencerate Tracker.[25] Audiencerate claims to anonymize the data and organizes it into segments.[26] Then, companies use the segmented data to run targeted campaigns
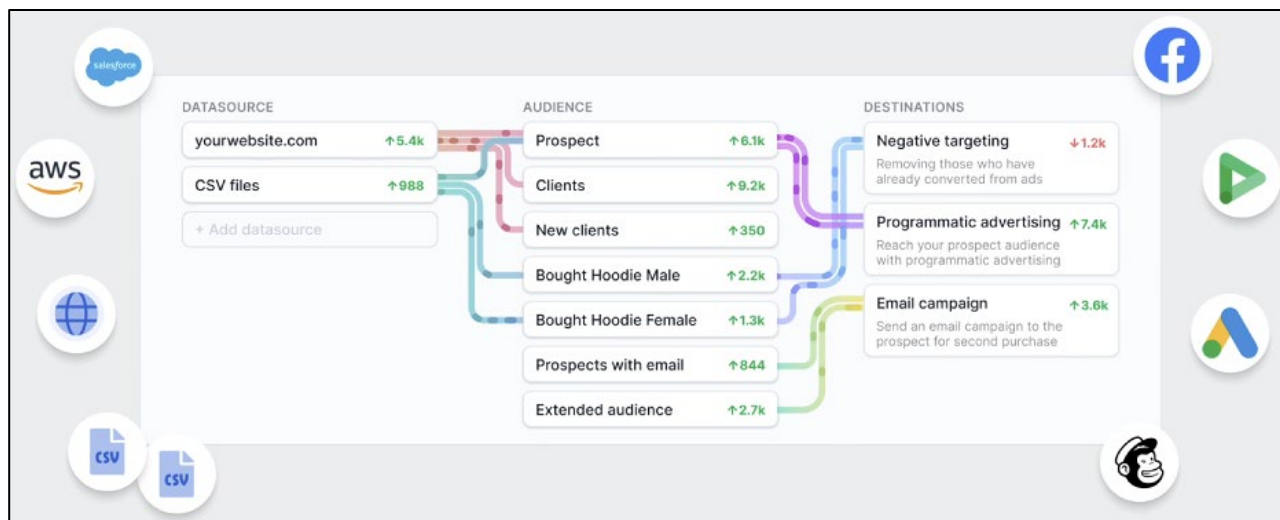
---

[24] AUDIENCERATE, https://www.audiencerate.com/ (last visited Jan. 4, 2024).

[25] AUDIENCERATE, https://www.audiencerate.com/ (last visited Jan. 3, 2024).

[26] *Product Overview*, AUDIENCERATE, https://app.audiencerate.com/doc/home (last visited Jan. 3, 2024).

and perform data analysis through Audiencerate's platform.[27] *See* Figure 11.

Figure 11:

84.   In addition to helping companies make better use of their own customer data, Audiencerate helps companies *sell* their customers' data to further "monetize data."[28]

85.   In order to perform the functions listed above, Audiencerate needs to collect data that identifies a particular user. This is why Audiencerate collects IP addresses: it allows Audiencerate to segment users in order to run targeted campaigns and perform data analysis.

86.   In other words, companies like Defendant are collecting users' data and sending it to Audiencerate for a profit, whether it is by optimizing marketing campaigns or by purely selling the data.

III.   PLAINTIFF'S EXPERIENCE

87.   Plaintiff has visited the Website multiple times—including as long ago as February 2023 and as recently as January 2024—on her desktop browser.

88.   When Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the Trackers to be installed on Plaintiff's browser. Defendant, TripleLift,

---

[27] *Id.*

[28] *Audiencerate partnership sees Sirdata integrated on Adform marketplace for the first time*, SIRDATA (Dec. 10, 2020), https://news.sirdata.com/en/press-release-audiencerate-sirdata-partnership/.

GumGum, and Audiencerate, then used the Trackers to collect Plaintiff's IP address. *See* Figures 12 (TripleLift Tracker), 13 (GumGum Tracker) and 14 (Audiencerate Tracker).
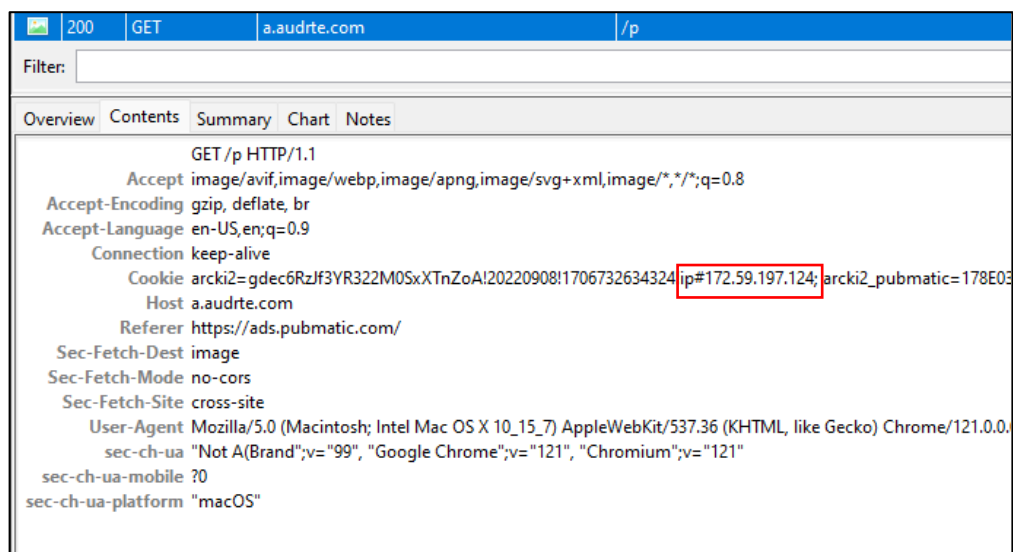
Figure 12:

Figure 13:

Figure 14:

89.   Because Plaintiff had previously visited the Website but did not clear her cookies at the time the data in Figures 12 and 13 were collected, Plaintiff's IP address was sent to TripleLift and GumGum with the TripleLift and GumGum cookies, as opposed to being sent as standalone data as it would have been on Plaintiff's first visit to the Website. *See* Figures 3 and 4, *supra*.

90.   Defendant, TripleLift, GumGum, and Audiencerate used the information collected by the Trackers to analyze Website data and marketing campaigns, conduct targeted advertising, and ultimately boost Defendant's and advertisers' revenue.

91.   Plaintiff did not provide her prior consent to Defendant to install or use the Trackers on her browser.

92.   Defendant did not obtain a court order before installing or using the Trackers.

93.   Plaintiff's privacy, therefore, was invaded by Defendant's violations of CIPA § 638.51(a).

CLASS ALLEGATIONS

94.   Pursuant to Cal. Code Civ. Proc. § 382, Plaintiff seeks to represent a class defined as all California residents who accessed the Website in California and had their IP address collected by the Trackers (the "Class").

95.   The following people are excluded from the Class: (i) any Judge presiding over this action and members of her or her family; (ii) Defendant, Defendant's subsidiaries, parents,

successors, predecessors, and any entity in which Defendant or their parents have a controlling interest (including current and former employees, officers, or directors); (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff's counsel and Defendant's counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

96.   **Numerosity:** The number of people within the Class is substantial and believed to amount to thousands, if not millions of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

97.   **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary between members of the Class, 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 violated CIPA § 638.51(a);

(b)   Whether the Trackers are "pen registers" pursuant to Cal. Penal Code §§ 638.50(b);

(c)   Whether Defendant sought or obtained prior consent—express or otherwise—from Plaintiff and the Class;

(d)   Whether Defendant sought or obtained a court order for its use of the Trackers; and

(e)   Whether Plaintiff and members of the Class are entitled to actual and/or statutory damages for the aforementioned violations.

98.   **Typicality:** The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other members of the Class Members, visited the Website and had her IP address collected by the Trackers, which were installed and used by Defendant.

99.   **Adequate Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class Members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiff and her counsel.

100.   **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Class. Each individual member of the Class may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability.   Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

COUNT I
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 638.51(a)

101.   Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

103.   CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

104.   A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or

electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

105. The Trackers are "pen registers" because they are "device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information"—the IP address—from the electronic communications transmitted by Plaintiff's and the Class's computers or smartphones. Cal. Penal Code § 638.50(b).

106. At all relevant times, Defendant installed the Trackers—which are pen registers—on Plaintiff's and Class Members' browsers, and used the Trackers to collect Plaintiff's and Class Members' IP address.

107. The Trackers do not collect the content of Plaintiff's and the Class's electronic communications with the Website. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication…") (cleaned up).

108. Plaintiff and Class Members did not provide their prior consent to Defendant's installation or use of the Trackers.

109. Defendant did not obtain a court order to install or use the Trackers.

110. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a)   For an order certifying the Class, naming Plaintiff as the representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b)   For an order declaring that Defendant's conduct violates the statutes referenced herein;

(c)   For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d)   For statutory damages of $5,000 for each violation of CIPA § 638.51(a);

(e)   For pre- and post-judgment interest on all amounts awarded;

(f)   For an order of restitution and all other forms of equitable monetary relief; and

(g)   For an order awarding and the Class their reasonable attorney's fees and expenses and costs of suit.

<u>DEMAND FOR JURY TRIAL</u>

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Dated: February 12, 2024   Respectfully submitted,

BURSOR & FISHER, P.A.

By:_____
                Emily A. Horne

L. Timothy Fisher (State Bar No. 191626)
Emily A. Horne (State Bar No. 347723)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
              ehorne@bursor.com

Attorneys for Plaintiff