

1 Rafey Balabanian (SBN 315962)  
rbalabanian@edelson.com  
2 Jared Lucky (SBN 354413)  
jlucky@edelson.com  
3 EDELSON PC  
150 California Street, 18th Floor  
4 San Francisco, California 94111  
Tel: 415.212.9300  
5 Fax: 415.373.9435

6 Schuyler Ufkes\*  
sufkes@edelson.com  
7 EDELSON PC  
350 North LaSalle Street, 14th Floor  
8 Chicago, Illinois 60654  
Tel: 312.589.6370  
9 Fax: 312.589.6378

10 *\*Pro hac vice admission to be sought*

11 *Counsel for Plaintiff and the Putative Class*

12 **IN THE UNITED STATES DISTRICT COURT**  
13 **FOR NORTHERN DISTRICT OF CALIFORNIA**  
14 **SAN JOSE DIVISION**

15 ALEX WOODS, individually and on behalf  
of all others similarly situated,

16 *Plaintiff,*

17 v.

18 VERVE GROUP, INC., a Delaware  
corporation,

19 *Defendant.*

Case No.:

**CLASS ACTION COMPLAINT FOR:**

- (1) Violation of Cal. Penal Code § 638.51;**
- (2) Violation of Cal. Penal Code § 502;**
- and**
- (3) Violation of Cal. Penal Code § 631.**

**AND DEMAND FOR JURY TRIAL**

22 Plaintiff Alex Woods (“Plaintiff” or “Woods”) brings this Class Action Complaint and  
23 Demand for Jury Trial against Verve Group, Inc. (“Verve” or “Defendant”) for surreptitiously  
24 tracking and selling California residents’ sensitive movements and locations. Plaintiff alleges as  
25 follows upon personal knowledge as to himself and his own acts and experiences, and, as to all  
26 other matters, upon information and belief.

**NATURE OF THE ACTION**

1  
2 1. Defendant Verve is an ad tech company and a data aggregator that surreptitiously  
3 collects and sells information about consumers from their mobile devices.

4 2. Verve developed and disseminated a software development kit (“SDK”) that enables  
5 backdoor access to consumers’ devices and opens a direct data collection pipeline to Verve and its  
6 advertising platform monetization partners. Thousands of developers have embedded Verve’s SDK  
7 into their mobile apps, allowing them to siphon data from more than 2 billion consumer devices  
8 around the world.

9 3. The data that Verve collects from unsuspecting consumers is incredibly sensitive.  
10 Verve collects timestamped geolocation data that reveals where a consumer lives and works, and  
11 which locations they frequent. The collected location data reveals sensitive information about each  
12 consumer, such as their religious affiliation, sexual orientation, and medical conditions. This  
13 enormous volume of data enables Verve and its monetization partners to build and sell  
14 comprehensive profiles of each consumer that includes their movements and whereabouts.

15 4. Verve ensures that none of the data it collects from consumers’ devices remains  
16 anonymous. By using its “identity graphs” process, Verve ingests and analyzes what it describes as  
17 a “treasure trove of identifiers” it obtained from mobile apps and third-party data providers to not  
18 only create a comprehensive profile on a consumer but also cross-reference and correlate various  
19 device identifiers with personal information to ascertain a consumer’s identity.

20 5. Plaintiff and the putative Class are consumers whose sensitive data, including their  
21 location data, has been collected by Verve in violation of Cal. Penal Code § 638.51, Cal. Penal  
22 Code § 502, and Cal. Penal Code § 631. Neither Plaintiff nor any member of the putative Class has  
23 ever agreed to allow Verve to collect or sell their sensitive data and there is no mechanism to opt  
24 out of Verve’s data collection practices.

**PARTIES**

25  
26 6. Plaintiff Alex Woods is a natural person and citizen of the State of California.

27 7. Defendant Verve Group, Inc. is a corporation organized and existing under the laws

1 of Delaware with its principal place of business located at 350 5th Avenue, Suite 7700, New York,  
2 New York 10118.

3 **JURISDICTION AND VENUE**

4 8. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)  
5 because (i) at least one member of the Class is a citizen of a different state than any Defendant, (ii)  
6 the amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and (iii) none of  
7 the exceptions under that subsection apply to this action.

8 9. This Court has personal jurisdiction over Defendant because Defendant conducts  
9 business in this District, including, on information and belief, contracting with Ifwe, Inc.—which  
10 is also headquartered in California—to embed Defendant’s SDK into the Tagged app. Further, a  
11 substantial part of the events or omissions giving rise to Plaintiff’s claims occurred in the District.

12 10. Venue is proper pursuant to 28 U.S.C. § 1391(b) because Plaintiff resides in this  
13 District and a substantial part of the events or omissions giving rise to Plaintiff’s claims occurred  
14 in the District.

15 **DIVISIONAL ASSIGNMENT**

16 11. Pursuant to Civil Local Rule 3-2(c)–(d), this case should be assigned to the San  
17 Jose Division because a substantial part of the events or omission giving rise to the claim occurred  
18 within the county of Santa Clara.

19 **COMMON FACTUAL ALLEGATIONS**

20 ***Verve Surreptitiously Collects Precise Location Information from Billions of Mobile Devices***

21 12. Verve Group is an ad tech company and a data aggregator. Their business model is  
22 to collect information from consumers, repackage and append the information, and sell access to its  
23 ill-gotten data to advertisers as well as other data brokers. Among the sensitive data Verve collects  
24 from consumers is timestamped geolocation data.

25 13. The secret to Verve’s data pipeline is the collection of what the ad industry calls  
26 “first-party data,” or data collected directly from consumers. Verve accomplishes this task by  
27 developing a SDK called “PubNative.”

1           14.     SDKs are a collection of reusable and packaged pieces of computer code that  
2 perform specific functions and processes. Software developers can integrate SDKs into their  
3 applications to save time and execute specific tasks.

4           15.     Various developers have integrated Defendant’s PubNative SDK into their mobile  
5 apps. On information and belief, over five thousand mobile apps have embedded Verve’s SDK.  
6 These apps include, among others, productivity, dating, photography, and gaming apps. Verve’s  
7 parent company claims that its SDK is on over 2 billion devices worldwide.

8           16.     Verve surreptitiously collects sensitive data from consumers through its PubNative  
9 SDK. Verve collects precise and timestamped latitude and longitude geolocation coordinates from  
10 consumers’ devices, mobile advertising IDs (“MAIDs”), the mobile app name, and device  
11 fingerprint data.

12           17.     Device fingerprint data includes information about the consumer’s hardware and  
13 software such as their device make and model, their device’s screen resolution, current operating  
14 system version, the amount of available and used disk space on their device, and battery level,  
15 among others.

16           18.     The problem with Verve’s SDK is that consumers do not know that by interacting  
17 with an app which has embedded the PubNative SDK that their sensitive data is being  
18 surreptitiously siphoned off by an unknown third party. Consumers are never informed about  
19 Verve’s SDK nor are they allowed to opt-in or opt-out of Verve’s data collection practices—if they  
20 even know who or what PubNative and Verve are.

21           19.     Indeed, when enabling location services within an app—for example a dating app or  
22 a weather app that necessarily requires the consumer to share his or her location *with the app*—the  
23 consumer grants consent *for only the mobile app* to use his or her location. At no point does Verve  
24 inform consumers that its SDK is collecting their sensitive geolocation data, nor does it prompt  
25 consumers to grant Verve permission to access or collect any data whatsoever.

1           20.     On information and belief, a consumer would never know that any given app has the  
2 PubNative SDK third-party tracking software embedded. The entire data collection process takes  
3 place surreptitiously without the consumer’s knowledge or consent.

4 ***Verve Ensures that Collected Consumer Data Does Not Remain Anonymous***

5           21.     As a preliminary matter, geolocation information is sensitive data that necessarily  
6 reveals a consumer’s identity. Geolocation coordinates together with timestamp data—exactly the  
7 type of data Defendant Verve collects through its PubNative SDK—can reveal a consumer’s home  
8 address, work address, and any other location they visit.

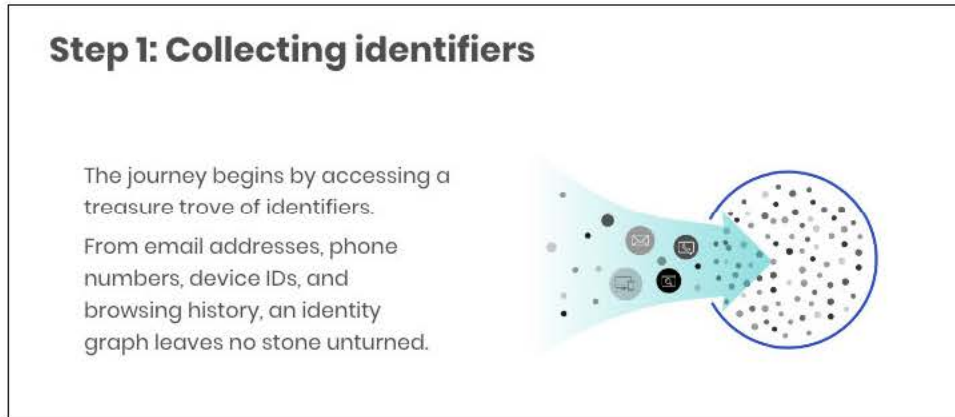
9           22.     Indeed, researchers from MIT found that a small location data sample is sufficient to  
10 identify an individual. The researchers analyzed timestamped location data for 1.5 million  
11 individuals over 15 months and found that only four timestamped locations are sufficient to identify  
12 95% of individuals. Given 11 data points, the researchers could identify all individuals in the study.  
13 The reason for the findings is obvious: individuals have unique movement patterns, and it is not  
14 likely that someone else will be in the same locations at four different times of the day.

15           23.     The researchers commented that an individual may be identified with less than four  
16 data points simply by exploiting irregularities in an individual’s behavior.

17           24.     By collecting timestamped geolocation data, MAIDs, and device fingerprint data,  
18 Verve can connect an ostensibly “anonymous” ID (such as a MAID) to an individual and then  
19 collect data on their interests and activities across the internet.

20           25.     Verve touts that it uses a technology it calls “identity graphs” to identify consumers  
21 across various platforms and screens. Verve states that its identity graphs technology is the reason  
22 behind “emails that address you by your first name to ads that eerily know your shopping  
23 preferences.” It explains, “an identity graph is like a digital Rolodex, but incredibly smarter. It is an  
24 online database that meticulously stores identifiers tied to individual customers and prospects,  
25 providing businesses with a 360-degree view of their audiences across diverse channels.”

1 26. Verve explains how its identity graphs technology works. First, Verve “begins by  
 2 accessing a treasure trove of identifiers. From email addresses, phone numbers, device IDs, and  
 3 browsing history, an identity graph leaves no stone unturned.” See Figure 1.



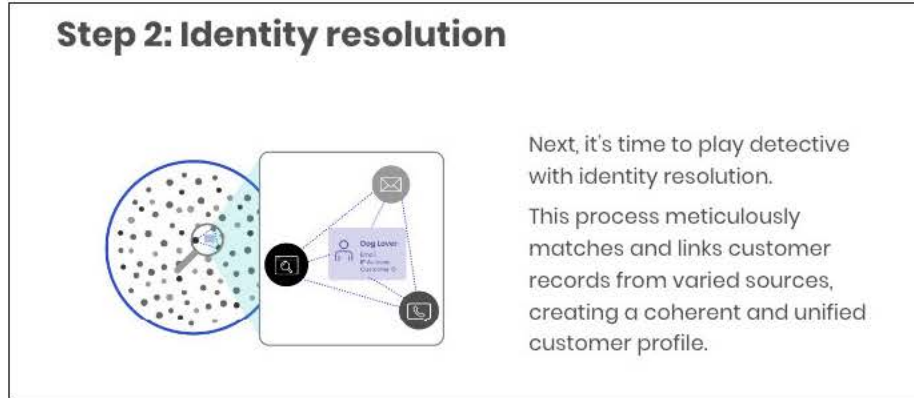
4  
5  
6  
7  
8  
9  
10  
11 **(Figure 1** showing Verve’s collection of “a treasure trove of identifiers.”)

12 27. As discussed above, Verve collects various identifiers such as MAIDs, timestamped  
 13 geolocation information, device fingerprint information, as well as information about their app  
 14 usage and online activities. Furthermore, Verve purports to obtain even more data from third-party  
 15 data providers such as Comcast, Oracle, and ID5, among others. See Figure 2. ID5, for example, is a  
 16 company that “provides identification services” and promises to provide its customers (like Verve)  
 17 “comprehensive identification capabilities.”



18  
19  
20  
21  
22  
23  
24 **(Figure 2)**

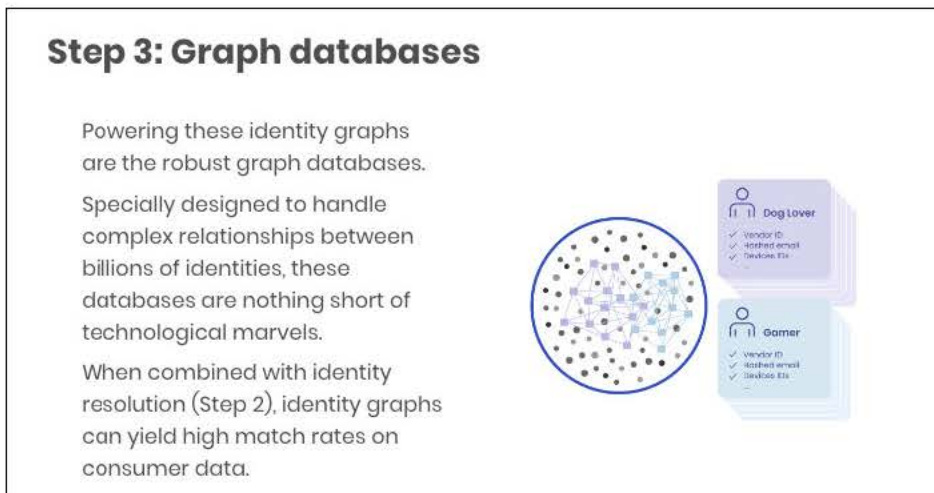
25 28. The second step of Verve’s identity graph is its “identity resolution” step that  
 26 “meticulously matches and links customer records from varied sources, creating a coherent and  
 27 unified customer profile.” See Figure 3.



**(Figure 3)**

29. Verve plays “detective” by matching various identifiers it has obtained directly from a consumer with data it bought from third-party providers to create a profile on the consumer. For example, Verve can cross-reference a record of a consumer having visited a specific location with a record of a consumer having downloaded a certain app because both records share a common device ID.

30. The third step of Verve’s identity graph is to store the various links and relationships it has matched into a database. This database is “specially designed to handle complex relationships between billions of identities” and “can yield high match rates on consumer data.” See Figure 4.



**(Figure 4)**

31. Most importantly, Verve collects and updates its identity graphs database in real time. That means should a consumer change his or her MAID, for example, Verve will be able to continue to identify and track the consumer. Similarly, should a consumer download a new app or

1 visit a new location, Verve’s identity graphs will immediately know and update its database. Verve  
2 states, “identity graphs ensure businesses have the freshest view of their customers by updating in  
3 real-time.”

4 ***Verve’s Data Collection Reveals Sensitive Information About Consumers***

5 32. Verve’s practice is far from inconsequential. Its surreptitious and routine collection  
6 of precise geolocation data reveals locations associated with medical care, reproductive health,  
7 religious worship, mental health, and temporary shelters, such as shelters for the homeless, domestic  
8 violence survivors, or other at-risk populations, and addiction recovery centers. As such, Verve’s  
9 data collection may reveal, for instance, a consumer’s religious affiliation, sexual orientation,  
10 medical condition, and even whether the consumer is part of an at-risk population.

11 33. Verve has fingerprinted consumers and has correlated a vast amount of personal  
12 information about them not only from its surreptitious SDK but also from third-party data brokers—  
13 entirely without consumers’ knowledge and consent. Verve has created profiles on consumers and  
14 its graph database holds information about consumers’ interests, the locations they have visited, and  
15 the names of apps they have downloaded.

16 34. To make matters worse, Verve monetizes and sells its collected data—specifically  
17 the timestamped geolocation data, MAIDS, and device fingerprint data—to advertising platforms  
18 and advertisers.

19 35. Verve has partnered with various advertising demand side platforms (or “DSPs”).  
20 DSPs are where advertisers and agencies go to purchase digital advertisement inventory. According  
21 to Verve, it has partnered with over 30 various DSPs which it considers its “monetization  
22 partners.”<sup>1</sup> Most concerning is that Verve purports to exchange “Precise Geographic Location Data”  
23 with its DSPs and, in turn, any advertiser who seeks to purchase advertisements and/or consumer  
24 data.

---

26 <sup>1</sup> *Monetization Partners*, PubNative, <https://pubnative.net/monetization-partners/> (last visited Aug.  
27 5, 2024).



1           36.     Verve’s collection of sensitive geolocation data has enabled a host of third parties  
2 with access to such data to track consumers down to sensitive locations and track their every  
3 movement. Verve has not published a full list of third-party data purchasers, but the types of third  
4 parties benefiting from Verve’s data may include advertising agencies, Fortune 500 companies,  
5 advertising platforms, and even government agencies. Verve’s parent company claims that brands  
6 like McDonalds, Bank of America, Pepsico, Uber, and TikTok, among others, leverage Verve’s  
7 advertising (and tracking) capabilities.

8           37.     A government contractor named Mike Yeagley recently explained how the Pentagon  
9 finds its targets. Yeagley leveraged SDKs embedded in various mobile apps that transmit  
10 geolocation data to advertisement networks to obtain near real-time coordinates on his targets.  
11 Furthermore, Yeagley created geofences around government buildings to identify which devices—  
12 and subsequently which individuals—visited what building, where these individuals went  
13 afterwards, and with whom they associated.

14           38.     Yeagley’s use of the data shows not only how the United States might deploy this  
15 technology to track consumers, but also how this easily accessible location data could allow  
16 America’s adversaries to purchase the same type of information and use it to track American  
17 residents.

18           39.     The Defense Intelligence Agency (“DIA”) and the National Security Agency  
19 (“NSA”) have also previously purchased geolocation data surreptitiously collected from American  
20 consumers’ devices. Similarly, the Department of Homeland Security (“DHS”) has purchased more  
21 than 200 licenses since 2019 from vendors who broker location data from consumer devices.

22           40.     Ron Wyden, a senator from Oregon, in a letter to the FTC, has harshly criticized the  
23 practice of government agencies purchasing geolocation data on American consumers and blamed  
24 advertisers and developers for failing to disclose such data collection practices: “App developers  
25 and advertising companies did not meaningfully disclose to users their sale and sharing of personal  
26 data with data brokers nor seek to obtain informed consent.”  
27

1 41. Ultimately, the PubNative SDK has allowed Verve to secretly create a detailed log of  
2 Plaintiff's and the putative Class's precise movement patterns, along with a dossier of their likes  
3 and interests, all without their consent or permission.

4 **FACTS SPECIFIC TO PLAINTIFF**

5 42. Plaintiff Woods downloaded and used the "Tagged" dating app on his Android  
6 device within the last year.

7 43. To use the "Tagged" mobile app, Plaintiff enabled location services for the sole  
8 purpose of sharing his location with "Tagged." The developers of the "Tagged" mobile app have  
9 embedded the PubNative SDK into their mobile app, allowing Defendant to collect Plaintiff's  
10 timestamped geolocation information, device IDs, device fingerprint data, and information about  
11 which app(s) he uses on his mobile device.

12 44. Plaintiff did not (and could not) grant Defendant permission to collect any  
13 information—especially not precise geolocation information—from his device whatsoever.

14 **CLASS ACTION ALLEGATIONS**

15 45. **Class Definition:** Plaintiff Alex Woods brings this proposed class action pursuant to  
16 Federal Rule of Civil Procedure 23(b)(2) and Rule 23(b)(3) on behalf of himself and a Class of  
17 others similarly situated, defined as follows:

18 All California residents who downloaded and used an app on their mobile device (1) with  
19 the PubNative SDK embedded into the app and (2) that did not publicly disclose "Verve" or  
20 "PubNative" in any of the app's notices or disclosures.

21 Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and  
22 members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors,  
23 predecessors, and any entity in which Defendant or its parents have a controlling interest and its  
24 officers and directors; (3) persons who properly execute and file a timely request for exclusion from  
25 the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or  
26 otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal  
27 representatives, successors, and assigns of any such excluded persons.

1           46.     **Numerosity:** The exact number of Class members is unknown and not available to  
2 Plaintiff at this time, but it is clear that individual joinder is impracticable. On information and  
3 belief, Defendant has surreptitiously collected timestamped geolocation information from millions  
4 of consumers who fall into the definition of the Class. Class members can be identified through  
5 Defendant's records.

6           47.     **Commonality and Predominance:** There are many questions of law and fact  
7 common to the claims of Plaintiff and the putative Class, and those questions predominate over any  
8 questions that may affect individual members of the Class. Common questions for the Class  
9 include, but are not necessarily limited to the following:

- 10                   (a)     Whether Defendant used a pen register;
- 11                   (b)     Whether Defendant obtained consent from Plaintiff and the Class or  
12                                 otherwise obtained a warrant to install and use a pen register;
- 13                   (c)     Whether Defendant accessed Plaintiff's and the Class's computer systems;
- 14                   (d)     Whether Defendant made an unauthorized connection with Plaintiff's and the  
15                                 Class's mobile devices; and
- 16                   (e)     Whether Defendant used or attempted to use any information obtained from  
17                                 Plaintiff's and the Class's mobile devices.

18           48.     **Typicality:** Plaintiff's claims are typical of the claims of the Class members in that  
19 Plaintiff, like all Class members, has been injured by Defendant's misconduct at issue.

20           49.     **Adequate Representation:** Plaintiff will fairly and adequately represent and protect  
21 the interests of the Class and has retained counsel competent and experienced in complex litigation  
22 and class actions. Plaintiff's claims are representative of the claims of the other members of the  
23 Class. That is, Plaintiff and the Class members sustained damages as a result of Defendant's  
24 conduct. Plaintiff also has no interests antagonistic to those of the Class, and Defendant has no  
25 defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this  
26 action on behalf of the members of the Class and have the financial resources to do so. Neither  
27 Plaintiff nor his counsel has any interest adverse to the Class.

1           50.     **Superiority:** Class proceedings are superior to all other available methods for the  
2 fair and efficient adjudication of this controversy, as joinder of all members of the Class is  
3 impracticable. Individual litigation would not be preferable to a class action because individual  
4 litigation would increase the delay and expense to all parties due to the complex legal and factual  
5 controversies presented in this Complaint. By contrast, a class action presents far fewer  
6 management difficulties and provides the benefits of single adjudication, economy of scale, and  
7 comprehensive supervision by a single court. Economies of time, effort, and expense will be  
8 fostered, and uniformity of decisions will be ensured.

9           51.     Plaintiff reserves the right to revise the foregoing “Class Allegations” and “Class  
10 Definition” based on facts learned through additional investigation and in discovery.

11  
12                                   **FIRST CAUSE OF ACTION**  
13                                   **Violation of California Invasion of Privacy Act**  
14                                   **Cal. Penal Code § 638.51**  
15                                   **(On behalf of Plaintiff and the Class)**

16           52.     Plaintiff incorporates the foregoing allegations as if fully set forth herein.

17           53.     California law prohibits the installation of a pen register without first obtaining a  
18 court order. Cal. Penal Code § 638.51.

19           54.     The statute defines a “pen register” as “a device or process that records or decodes  
20 dialing, routing, addressing, or signaling information transmitted by an instrument or facility from  
21 which a wire or electronic communication is transmitted, but not the contents of a communication.”  
22 Cal. Penal Code § 638.50(b).

23           55.     Defendant’s PubNative SDK is a “pen register” because it is a device or process that  
24 records addressing or signaling information—in this instance, Plaintiff’s and the Class members’  
25 location and personal information—from electronic communications transmitted by their devices.  
26 Furthermore, Defendant’s SDK is a device or process that identifies consumers, gathers data, and  
27 correlates data through sophisticated device fingerprinting and its “identity graph” functionality.

28           56.     Defendant was not authorized by any court order to use a pen register to track  
Plaintiff’s and Class members’ location and personal information, nor did it obtain consent from

1 Plaintiff and the Class to operate such a device.

2 57. Plaintiff and the Class seek injunctive relief and statutory damages in the amount of  
3 \$5,000 per violation pursuant to Cal. Penal Code § 637.2.

4  
5 **SECOND CAUSE OF ACTION**  
6 **Violation of the California Comprehensive Computer Data Access and Fraud Act**  
7 **Cal. Penal Code § 502**  
8 **(On behalf of Plaintiff and the Class)**

9 58. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

10 59. The California Legislature enacted the Comprehensive Computer Data Access and  
11 Fraud Act (“CDAFA”) to “expand the degree of protection afforded to individuals . . . from  
12 tampering, interference, damage, and unauthorized access to lawfully created computer data and  
13 computer systems.” Cal. Penal Code § 502(a). In enacting the statute, the Legislature emphasized  
14 the need to protect individual privacy: “[The] Legislature further finds and declares that protection  
15 of the integrity of all types and forms of lawfully created computers, computer systems, and  
16 computer data is vital to the protection of the privacy of individuals[.]” *Id.*

17 60. Plaintiff’s and the Class members’ mobile devices are “computers” or “computer  
18 systems” within the meaning of § 502(b) because they are devices capable of being used in  
19 conjunction with external files and perform functions such as logic, arithmetic, data storage and  
20 retrieval, and communication.

21 61. Defendant violated the following sections of CDAFA § 502(c):

22 a. “Knowingly accesses and without permission . . . uses any data, computer,  
23 computer system, or computer network in order to . . . wrongfully control or obtain  
24 money, property, or data.” *Id.* § 502(c)(1).

25 b. “Knowingly accesses and without permission takes, copies, or makes use of  
26 any data from a computer, computer system, or computer network.” *Id.* § 502(c)(2).

27 c. “Knowingly and without permission accesses or causes to be accessed any  
28 computer, computer system, or computer network.” *Id.* § 502(c)(7).

62. Defendant “accessed” Plaintiff’s and the Class members’ computers and/or computer

1 systems because it gained entry to and/or caused output from their mobile devices to obtain  
2 geolocation information and personal information.

3 63. Defendant was unjustly enriched with the data it obtained from Plaintiff and the  
4 Class.

5 64. Plaintiff and the Class now seek compensatory damages, injunctive relief,  
6 disgorgement of profits, other equitable relief, punitive damages, and attorneys' fees pursuant to §  
7 502(e)(1)–(2).

8 **THIRD CAUSE OF ACTION**  
9 **Violation of California Wiretap Act**  
10 **Cal. Penal Code § 631**  
11 **(On behalf of Plaintiff and the Class)**

12 65. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

13 66. The California Wiretap Act, Cal. Penal Code § 631, prohibits:

14 Any person [from using] any machine, instrument, or contrivance, or in any  
15 other manner . . . [from making] any unauthorized connection, whether  
16 physically, electrically, acoustically, inductively, or otherwise, with any  
17 telegraph or telephone wire, line, cable, or instrument, including the wire,  
18 line, cable, or instrument of any internal telephonic communication system,  
19 or who willfully and without the consent of all parties to the communication,  
20 or in any unauthorized manner, reads, or attempts to read, or to learn the  
21 contents or meaning of any message, report, or communication while the  
22 same is in transit or passing over any wire, line, or cable, or is being sent  
23 from, or received at any place within this state; or who uses, or attempts to  
24 use, in any manner, or for any purpose, or to communicate in any way, any  
25 information so obtained, or who aids, agrees with, employs, or conspires  
26 with any person or persons to unlawfully do, or permit, or cause to be done  
27 any of the acts or things mentioned above in this section[.]

28 67. Defendant's SDK tracked Plaintiff's and Class members' specific input events and  
choices on their mobile devices such as their movements and affirmative actions such as installing a  
mobile app on their device and therefore constitute communications within the scope of the  
California Wiretap Act.

68. Defendant's PubNative SDK made an unauthorized connection with Plaintiff's and  
Class members' devices and obtained their sensitive information including their movements,  
geolocation information, mobile device IDs, device fingerprint data, and information about the  
mobile app(s) they downloaded.



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

Jared Lucky (SBN 354413)  
jlucky@edelson.com  
EDELSON PC  
150 California Street, 18th Floor  
San Francisco, California 94111  
Tel: 415.212.9300  
Fax: 415.373.9435

Schuyler Ufkes\*  
sufkes@edelson.com  
EDELSON PC  
350 North LaSalle Street, 14th Floor  
Chicago, Illinois 60654  
Tel: 312.589.6370  
Fax: 312.589.6378

*\*Pro hac vice admission to be sought  
Counsel for Plaintiff and the Putative Class*



# ClassAction.org

This complaint is part of ClassAction.org's searchable [class action lawsuit database](#)

---