

BURSOR & FISHER, P.A.

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

BURSOR & FISHER, P.A.

Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

Attorneys for Plaintiff

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

AUTRY WILLIS, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

INMARKET MEDIA, LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Autry Willis (“Plaintiff”) by and through her attorneys, makes the following
2 allegations pursuant to the investigation of her counsel and based upon information and belief, except
3 as to allegations specifically pertaining to herself and her counsel, which are based on personal
4 knowledge, against Defendant InMarket Media, LLC. (“InMarket” or “Defendant”).

5 **NATURE OF THE ACTION**

6 1. InMarket violates state law by first acquiring and tracking consumers’ precise
7 geolocation data and other data through the use of spyware called “InMarket SDK” and then profiting
8 from that data by selling it to others. The data can include consumers’ movements to and from
9 sensitive locations, like locations associated with medical care, reproductive health, religious
10 worship, mental health, rallies, demonstrations, or protests.

11 2. Plaintiff is an individual who asserts claims on behalf of herself and other similarly
12 situated individuals for unjust enrichment and violations of California privacy statutes.

13 3. By selling this data without consent, Defendant has been unjustly enriched and has
14 violated Plaintiff’s privacy rights, state consumer protection and privacy statutes.

15 **PARTIES**

16 4. Plaintiff Autry Willis is a resident of Oakland, California. Plaintiff downloaded a
17 third-party phone application which contained geolocation data tracking using Defendant’s InMarket
18 SDK (the “App”). At the time, Plaintiff believed that the App would not transfer Plaintiff’s
19 geolocation data to another entity for the purposes of selling said data. However, that was not the
20 case: the App sent location data to Defendant when Plaintiff used the App. During that entire time,
21 the App tracked the geolocation of Plaintiff. In turn, Defendant tracked Plaintiff’s geolocation in
22 California, and then sold that data for profit. Plaintiff suffered her primary injury in California.
23 Plaintiff most recently used the App in or around December 2023.

24 5. During the time while Plaintiff used the App, Defendant took Plaintiff’s geolocation
25 data from the App and then sold Plaintiff’s location data to other third parties.

26 6. Plaintiff has not consented to have her geolocation data sold to third parties for
27 valuable consideration. If Plaintiff had been aware that Defendant would receive and sell her
28 geolocation data to third parties, Plaintiff would have not used the App.

1 17. Apps that incorporate the InMarket SDK request access to the location data generated
2 by a mobile device’s operating system.

3 18. Critically, if the user allows access, the InMarket SDK receives the device’s precise
4 latitude and longitude, along with a timestamp and unique mobile device identifier, as often as the
5 mobile device’s operating system provides it— ranging from almost no collection when the device
6 is idle, to every few seconds when the device is actively moving—and transmits it directly to
7 Defendant’s servers.

8 19. As a result, from 2016 to the present, about 100 million unique devices sent Defendant
9 location data *each year*.

10 20. Defendant collects sensitive information from consumers, including where they live,
11 where they work, where they worship, where their children go to school or obtain child care, where
12 they received medical treatment (potentially revealing the existence of medical conditions), whether
13 they went to rallies, demonstrations, or protests (potentially revealing their political affiliations), and
14 any other information that can be gleaned from tracking a person’s day-to-day movements.

15 21. This information is collected with several identifiers (including a unique mobile
16 device identifier). Defendant has retained this information for up to five years.

17 **B. Defendant Monetizes Users’ Location Data Through Targeted Advertising**

18 22. Defendant sorts consumers based on their visits to points of interest into audience
19 segments to which it can target advertising.

20 23. Defendant has created or maintains almost two thousand distinct advertising audience
21 segments.

22 24. For example, an InMarket brand client can target shoppers who are likely to be low-
23 income millennials; well-off suburban moms; parents of preschoolers, high-school students, or kids
24 who are home-schooled; Christian church goers; convenience-sensitive or price-sensitive; single
25 parents or empty-nesters; affluent savers or blue collar workers; “healthy or wealthy” or “wealthy
26 and not healthy,” to name only a selection of the categories InMarket offers or has offered to its
27 brand clients.
28

1 25. InMarket classifies audiences based on both past behavior and predictions it makes
2 about consumers based on that behavior.

3 26. For example, if a consumer’s past location data shows that she has visited a car
4 dealership, InMarket can combine that information with the consumer's attributes purchased from
5 other sources (age, income, family structure, education level), and can potentially predict that she
6 may be in the market for a certain type of vehicle.

7 27. The InMarket SDK displays the ads and determines which ads appear in which apps
8 incorporating the SDK.

9 28. Defendant additionally offers advertisers a product that sends push notifications based
10 on a consumer’s location and “geofencing,” the creation of a virtual fence around a particular point
11 of interest. When the InMarket SDK transmits a location that is inside a virtual fence, the app will
12 send a push notification for a particular ad.

13 29. For example, a consumer who is within 200 meters of a pharmacy might see an ad for
14 toothpaste, cold medicine, or some other product sold at that location.

15 30. Finally, Defendant also makes its advertising audience segments available on real-
16 time bidding platforms. An advertiser using one of these platforms can select an advertising
17 audience, and identify the amount that it is willing to pay (that is, its bid) each time its ad appears on
18 a mobile device that is a part of that audience.

19 31. The advertiser’s ad will appear on a particular device if it has the highest bid for that
20 device.

21 32. Defendant receives some revenue each time an advertiser uses one of its audiences in
22 this process.

23 C. **Defendant Fails To Verify That Users Of Third-Party Apps Incorporating**
24 **InMarket’s SDK Have Been Notified That Their Location Data Will Be Used**
25 **To Target Advertising**

26 33. Defendant does little to verify that third-party apps incorporating its SDK obtain
27 informed consumer consent before granting InMarket access to their sensitive location data.

28 34. InMarket additionally neither collects nor retains records of the disclosures that third-
party apps incorporating the InMarket SDK provide consumers before accessing their location data.

1 35. In fact, InMarket does not require the third-party apps that incorporate its SDK to
2 obtain informed consumer consent.

3 36. Even if these third-party app developers wanted to provide adequate disclosure to
4 their users about InMarket’s use of their location data, InMarket does not provide the developers
5 with sufficient information to provide that notice.

6 37. Specifically, InMarket’s contract with third-party app developers merely states that
7 InMarket will serve ads on the developer’s apps in return for developers passing user information to
8 InMarket, including precise location and advertising identifiers.

9 38. Defendant does not disclose that information collected from these third-party users
10 will be supplemented and cross-referenced with purchased data and analyzed to draw inferences
11 about those users for marketing purposes.

12 39. Defendant therefore does not know whether users of hundreds of third-party apps that
13 incorporate the InMarket SDK were informed of their data being collected and used for targeted
14 advertising.

15 **D. Defendant’s Practices Cause and Are Likely to Cause Substantial Injury to**
16 **Consumers**

17 40. Because Defendant readily combined the location data of those users into its
18 databases and systems without confirming user consent, Defendant obtained and used that data
19 without informed user consent, resulting in consumer injury.

20 41. In addition, after collecting sensitive precise location data about consumers’ daily
21 movements, Defendant retains that information longer than reasonably necessary to accomplish the
22 purpose for which that information was collected and thereby exposes consumers to significant
23 unnecessary risk. Specifically, InMarket has retained consumer location data for five years prior to
24 deletion.

25 42. This unreasonably long retention period—significantly increases the risk that this
26 sensitive data could be disclosed, misused, and linked back to the consumer, thereby exposing
27 sensitive information about that consumer’s life.
28

1 43. Defendant’s comprehensive collection and long-term retention of location data
2 subjects consumers to a likelihood of substantial injury through the exposure of their re-identified
3 location.

4 **FTC’S JANAURY 2023 COMPLAINT AGAINST DEFENDANT**

5 44. In January 2023, the FTC took action against Defendant for allegations that are
6 substantially identical to this complaint.

7 45. According to the FTC’s complaint, Defendant’s acts as described above constitutes
8 a violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits “unfair or deceptive
9 acts or practices in or affecting commerce.”

10 46. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are
11 likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves
12 and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. §
13 45(n).

14 **CLASS ALLEGATIONS**

15 47. ***Class Definition.*** Plaintiff brings this action on behalf of a class of similarly
16 situated individuals, defined as all persons in the United States whose data, including but not limited
17 to their geolocation data, was sold by Defendant without their consent (the “Class”).

18 (a) ***California Subclass.*** Plaintiff also seeks to represent a subclass defined as
19 all Class members who reside in California whose data, including but not limited to
20 their geolocation data, was sold by Defendant without their consent (the “California
21 Subclass”).

22 48. Excluded from the Class and Subclass are Defendant and any entities in which
23 Defendant has a controlling interest, Defendant’s agents and employees, the judge to whom this
24 action is assigned, and members of the judge’s staff, and the judge’s immediate family.

25 49. Subject to additional information obtained through discovery, the foregoing class
26 definitions may be modified or narrowed by an amended complaint, or at class certification,
27 including through the use of multi-state subclasses to account for material differences in state law, if
28 any.

1 50. Members of the Class and California Subclass are so numerous that their individual
2 joinder herein is impracticable. On information and belief, members of the Class and California
3 Subclass number in the millions. The precise number of Class members and their identities are
4 unknown to Plaintiff at this time but may be determined through discovery. Class members may be
5 notified of the pendency of this action by mail and/or publication through the distribution records of
6 Defendant and third-party retailers and vendors.

7 51. Common questions of law and fact exist as to all Class members and predominate
8 over questions affecting only individual Class members. Common legal and factual questions
9 include but are not limited to whether Defendant's sale of geolocation data without consent
10 constitutes unjust enrichment.

11 52. The claims of the named Plaintiff are typical of the claims of the Class in that the
12 named Plaintiff's data was sold by Defendant without her consent, and the named Plaintiff suffered
13 injury as a result of Defendant's conduct.

14 53. Plaintiff is an adequate representative of the Class and California Subclass because
15 her interests do not conflict with the interests of the Class members she seeks to represent, she has
16 retained competent counsel experienced in prosecuting class actions, and she intends to prosecute
17 this action vigorously. The interests of Class members will be fairly and adequately protected by
18 Plaintiff and her counsel.

19 54. The class mechanism is superior to other available means for the fair and efficient
20 adjudication of the claims of Class members. Each individual Class member may lack the resources
21 to undergo the burden and expense of individual prosecution of the complex and extensive litigation
22 necessary to establish Defendant's liability. Individualized litigation increases the delay and expense
23 to all parties and multiplies the burden on the judicial system presented by the complex legal and
24 factual issues of this case. Individualized litigation also presents a potential for inconsistent or
25 contradictory judgments. In contrast, the class action device presents far fewer management
26 difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive
27 supervision by a single court on the issue of Defendant's liability. Class treatment of the liability
28

1 issues will ensure that all claims and claimants are before this Court for consistent adjudication of
2 the liability issues.

3 **COUNT I**
4 **Invasion of Privacy**

5 55. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

6 56. Plaintiff brings this claim individually and on behalf of the California Subclass.

7 57. The California Constitution recognizes the right to privacy inherent in all residents of
8 the State and creates a private right of action against private entities that invade that right.

9 58. Article I, Section 1 of the California Constitution provides: “All people are by nature
10 free and independent and have inalienable rights. Among these are enjoying and defending life and
11 liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness,
12 and privacy.”

13 59. The right to privacy was added to the California Constitution in 1972, through
14 Proposition 11 (called the “Right to Privacy Initiative”). Proposition 11 was designed to codify the
15 right to privacy, protecting individuals from invasions of privacy from both the government and
16 private entities alike: “The right of privacy is the right to be left alone. It is a fundamental and
17 compelling interest. ... It prevents government and business interests from collecting and stockpiling
18 unnecessary information about us and from misusing information gathered for one purpose in order
19 to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control
20 circulation of personal information.” Ballot Pamp., Proposed Stats. And Amends. To Cal. Const.
21 with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also*
22 *Hill v. Colorado*, 530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one’s
23 home from unwanted communication); *Hill v. National Collegiate Athletic Assn.* (1994), 7 Cal.4th
24 1, 81, (Mosk, J., dissenting).

25 60. Plaintiff and the California Subclass members have a legally protected privacy
26 interest, as recognized by the California Constitution, CIPA, common law and the 4th Amendment
27 to the United States Constitution.
28

1 61. Plaintiff and California Subclass members had a reasonable expectation of privacy
2 under the circumstances, as they could not have reasonably expected that Defendant would violate
3 state and federal privacy laws. Plaintiff and California Subclass members were not aware and could
4 not have reasonably expected that unknown third party would install software on their mobile devices
5 that would track and transmit their physical location and communications, and share Plaintiff's and
6 California Subclass members' sensitive information with other parties.

7 62. Defendant's conduct violates, at a minimum:

8 (a) The right to privacy in data, communications and personal information
9 contained on personal devices;

10 (b) The California Constitution, Article I, Section 1;

11 (c) The California Wiretapping Act;

12 (d) The California Invasion of Privacy Act; and

13 (e) The California Computer Data Access and Fraud Act.

14 63. Defendant's conduct in secretly intercepting and collecting Plaintiff's and California
15 Subclass members' personal information, location data, and communications is an egregious breach
16 of social norms and is highly offensive to a reasonable person.

17 64. Defendant's conduct in analyzing, using, and sharing with third parties the personal
18 information and communications that Defendant intercepted and took from Plaintiff's and California
19 Subclass members is an egregious breach of societal norms and is highly offensive to a reasonable
20 person, and violates Plaintiff's and California Subclass members' reasonable expectations of privacy.

21 65. Plaintiff and California Subclass members did not consent for Defendant to track,
22 collect, or use their personal information and communications.

23 66. As a direct and proximate result of Defendant's invasion of their privacy, Plaintiff and
24 California Subclass members were injured and suffered damages. Plaintiff and California Subclass
25 members are entitled to equitable relief and just compensation in an amount to be determined at trial.

26 67. Defendant was unjustly enriched as a result of its invasion of Plaintiff's and California
27 Subclass members' privacy.

COUNT II

**Violation of the California Computer Data Access and Fraud Act
*Cal. Penal Code. § 502***

68. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

69. Plaintiff brings this claim individually and on behalf of the California Subclass.

70. The California legislature enacted the CDAFA with the intent of “expand[ing] the degree of protection afforded to individuals ... from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.” Cal. Penal Code §502(a). The enactment of CDAFA was motivated by the finding that “the proliferation of computer technology has resulted in a concomitant proliferation of ... unauthorized access to computers, computer systems, and computer data.” *Id.*

71. Plaintiff’s and California Subclass members’ smartphone constitute “computers” within the scope of the CDAFA.

72. Defendant violated the following sections of the CDAFA:

(a) Section 502(c)(1), which makes it unlawful to “knowingly access[] and without permission ... use[] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;”

(b) section 502(c)(2), which makes it unlawful to “knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;”

(c) Section 502(c)(7), which makes it unlawful to “knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.”

73. Defendant knowingly accessed Plaintiff’s and California Subclass members’ smartphones without their permission by including within the SDK, that Defendant provides to developers, software that intercepts and transmits data, communications, and personal information concerning Plaintiff and California Subclass members.

1 74. Defendant used data, communications, and personal information that it intercepted
2 and took from Plaintiff's and California Subclass members' smart phones to wrongfully and unjustly
3 enrich itself at the expense of Plaintiff and California Subclass members.

4 75. Defendant took, copied, intercepted, and made use of data, communications, and
5 personal information from Plaintiff's and California Subclass members' smartphones.

6 76. Defendant knowingly and without Plaintiff's and California Subclass members'
7 permission accessed or caused to be their smartphones by installing without Plaintiff's and California
8 Subclass members' informed consent software that intercepts and/or takes data, communications,
9 and personal information concerning Plaintiff and California Subclass members.

10 77. Plaintiff and California Subclass members are residents of California, and used their
11 smartphones in California. Defendant accessed or caused to be accessed Plaintiff's and California
12 Subclass members' data, communications, and personal information from California. On
13 information and belief, Defendant uses servers located in California that allow Defendant to access
14 and process the data, communications and personal information concerning Plaintiff and California
15 Subclass Members.

16 78. Defendant was unjustly enriched by intercepting, acquiring, taking, or using
17 Plaintiff's and California Subclass members' data, communications, and personal information
18 without their permission, and using it for Defendant's own financial benefit. Defendant has been
19 unjustly enriched in an amount to be determined at trial.

20 79. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiff
21 and California Subclass Members suffered damages.

22 80. Pursuant to CDAFA Section 502(e)(1), Plaintiff and California Subclass Members
23 seek compensatory, injunctive and equitable relief in an amount to be determined at trial.

24 81. Pursuant to CDAFA Section 502(e)(2), Plaintiff and California Subclass Members
25 seek an award of reasonable attorney's fees and costs.

26 82. Pursuant to CDAFA Section 502(e)(4), Plaintiff and California Subclass Members
27 seek punitive or exemplary damages for Defendant's willful violations of the CDAFA.
28

COUNT III

**Use of a Pen Register or Trap and Trace Device
Cal. Penal Code § 638.51**

83. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

84. Plaintiff brings this claim individually and on behalf of the California Subclass against Defendant.

85. California Penal Code Section 638.50(b) defines a “pen register” as “a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.”

86. California Penal Code Section 638.51 prohibits any person from using a pen register without a court order.

87. Defendant’s SDK constitutes a “pen register” because it is a device or process that records addressing or signaling information—Plaintiff’s and California Subclass Members’ location data and personal information—from the electronic communications transmitted by their smartphones.

88. Defendant was not authorized by any court order to use a pen register to track Plaintiff’s and California Subclass members’ location data and personal information.

89. As a direct and proximate result of Defendant’s conduct, Plaintiff and California Subclass Members suffered losses and were damages in an amount to be determined at trial.

COUNT IV

**Violation of the California Wiretapping Act
Cal. Penal Code § 631**

90. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

91. Plaintiff brings this claim individually and on behalf of the California Subclass.

92. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

1 93. The California legislature enacted the California Invasion of Privacy Act (“CIPA”),
2 Cal. Penal Code § 630, *et seq.*, including the Wiretapping Act, “to protect the right of privacy” of
3 residents of California. Cal. Penal Code § 630.

4 94. The California legislature was motivated to enact CIPA by a concern that the
5 “advances in science and technology have led to the development of new devices and techniques for
6 the purpose of eavesdropping upon private communications and that the invasion of privacy resulting
7 from the continual and increasing use of such devices and techniques has created a serious threat to
8 the free exercise of personal liberties and cannot be tolerated in a free and civilized society.” *Id.*

9 95. The California Wiretapping Act prohibits:

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

22 96. Plaintiff’s and California Subclass Members’ specific user input events and choices
23 on their mobile devices that are tracked by Defendant’s SDK communicates the user’s affirmative
24 actions, such as clicking a link, installing an app, selecting an option, or relaying a response, and
25 constitute communications within the scope of the Wiretapping Act.

26 97. Plaintiff and California Subclass Members are residents of California, and used their
27 smartphones within California. As such, Defendant intercepts, reads, or attempts to read Plaintiff’s
28 and Class members’ data, communications, and personal information in California.

 98. On information and belief, Defendant uses servers in California to intercept, track,
process, or otherwise use Plaintiff’s and California Subclass members’ data, communications, and
personal information within California.

1 99. Defendant intercepts Plaintiff's and California Subclass Members' communications
2 while they are in transit to and from Plaintiff's and California Subclass Members' smartphones and
3 the apps, app developers, and cellphone towers; Defendant transmits a copy of Plaintiff's and
4 California Subclass Members' communications to itself. Defendant uses the contents of the
5 communications to sell to third parties and in other methods for its own pecuniary gain.

6 100. Neither Defendant nor any other person informed Plaintiff and California Subclass
7 members that Defendant was intercepting and transmitting Plaintiff's private communications.
8 Plaintiff and California Subclass Members did not know Defendant was intercepting and recording
9 their communications, as such they could not and did not consent for their communications to be
10 intercepted by Defendant and thereafter transmitted to others.

11 101. Defendant's SDK constitutes a machine, instrument, contrivance or other manner to
12 track and intercept Plaintiff's and California Subclass members' communications while they are
13 using their smartphones.

14 102. Defendant uses and attempts to use or communicate the meaning of Plaintiff's and
15 California Subclass members' communications by ascertaining their personal information, including
16 their geolocation and places that they have visited, in order to sell Plaintiff's and California Subclass
17 members' personal information to third parties.

18 103. At all relevant times to this complaint, Defendant intercepted and recorded
19 components of Plaintiff's and the putative California Subclass' private telephone communications
20 and transmissions when Plaintiff and other California Subclass Members accessed Defendant's
21 software via their cellular mobile access devices within the State of California.

22 104. At all relevant times to this complaint, Plaintiff and other California Subclass
23 Members did not know Defendant was engaging in such interception and recording and therefore
24 could not provide consent to have any part of their private and confidential video conferencing
25 communications intercepted and recorded by Defendant and thereafter transmitted to others.

26 105. At the inception of Defendant's illegally intercepted and stored her geolocation and
27 other personal data, Defendant never advised Plaintiff or the other California Subclass Members that
28 any part of this sensitive personal data would be intercepted, recorded and transmitted to third parties.

1 106. Section 631(a) is not limited to phone lines, but also applies to “new technologies”
2 such as computers, the Internet, and email.

3 107. Defendant’s use of its SDK is both a “machine, instrument, contrivance, or ... other
4 manner” used to engage in the prohibited conduct at issue here.

5 108. At all relevant times, by using Defendant’s SDK as well as tracking Plaintiff’s and
6 California Subclass Members’ geolocation, Defendant intentionally tapped, electrically or otherwise,
7 the lines of internet communication between Plaintiff and California Subclass Members on the one
8 hand, and the specific sites and locations Plaintiff and California Subclass Members visited on the
9 other.

10 109. At all relevant times, by using Defendant’s geolocation tracking software technology,
11 Defendant willfully and without the consent of all parties to the communication, or in any
12 unauthorized manner, read or attempted to read or learn the contents or meaning of electronic
13 communications of Plaintiff and putative California Subclass members, while the electronic
14 communications were in transit or passing over any wire, line or cable or were being sent from or
15 received at any place within California.

16 110. Plaintiff and California Subclass Members did not consent to any of Defendant’s
17 actions in implementing these wiretaps within its geolocation tracking software. Nor have Plaintiff
18 or California Subclass Members consented to Defendant’s intentional access, interception, reading,
19 learning, recording, and collection of Plaintiff and California Subclass Members’ electronic
20 communications.

21 111. Plaintiff’s and the California Subclass Members’ devices of which Defendant
22 accessed through its unauthorized actions included their computers, smart phones, and tables and/or
23 other electronic computing devices.

24 112. Defendant violated Cal. Penal Code § 631 by knowingly accessing and without
25 permission accessing Plaintiff and California Subclass Members’ devices in order to obtain their
26 personal information, including their device and location data and personal communications with
27 others, and in order for Defendant to share that data with third parties, in violation of Plaintiff’s and
28 California Subclass Members’ reasonable expectations of privacy in their devices and data.

1 113. Defendant violated Cal. Penal Code § 631 by knowingly and without permission
2 intercepting, wiretapping, accessing, taking and using Plaintiff’s and the California Subclass
3 Members’ personally identifiable information and personal communications with others.

4 114. As a direct and proximate result of Defendant’s violation of the Wiretapping Act,
5 Plaintiff and California Subclass Members were injured and suffered damages, a loss of privacy, and
6 loss of the value of their personal information in an amount to be determined at trial.

7 115. Defendant was unjustly enriched by its violation of the Wiretapping Act.

8 116. Pursuant to California Penal Code Section 637.2, Plaintiff and California Subclass
9 members have been injured by Defendant’s violation of the Wiretapping Act, and seek damages for
10 the greater of \$5,000 or three times the amount of actual damages, and injunctive relief.

11 **COUNT V**
12 **Unfair Practices**
13 **In Violation of the California Unfair Competition Law**
14 **Cal. Bus. & Prof. Code § 17200**

15 117. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

16 118. Plaintiff brings this claim individually and on behalf of the California Subclass.

17 119. At all relevant times there was in full force and effect the California Unfair
18 Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17200, *et seq.*, which prohibits, *inter alia*, “any
19 unlawful, *unfair*, or fraudulent business act or practice” and “unfair, deceptive, untrue, or misleading
20 advertising.” Cal. Bus. & Prof. Code § 17200 (emphasis added).

21 120. Defendant engaged in business acts and practices which are “unfair” under the UCL,
22 including surreptitiously collecting, tracking, using and disseminating Plaintiff’s and California
23 Subclass Members’ personal information, geolocation data, and communications.

24 121. Defendant also engaged in a number of practices designed to perpetuate the scheme
25 and the stream of revenue it generates. Those practices, which are unfair separately and particularly
26 when taken together, include but are not limited to invasion of Plaintiff’s and California Subclass
27 members’ privacy; surreptitiously tracking Plaintiff’s and California Subclass members’ location;
28 surreptitiously accessing Plaintiff’s and California Subclass members’ cellphones without
authorization; surreptitiously obtaining personal data from Plaintiff’s and California Subclass

1 members' cellphones; surreptitiously intercepting and recording Plaintiff's and California Subclass
2 members' communications.

3 122. Unfair acts under the UCL have been interpreted using three different tests: (1)
4 whether the public policy which is a predicate to a consumer unfair competition action under the
5 unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2)
6 whether the gravity of the harm to the consumer caused by the challenged business practice
7 outweighs the utility of the defendant's conduct; and (3) whether the consumer injury is substantial,
8 not outweighed by any countervailing benefits to consumers or competition, and is an injury that
9 consumers themselves could not reasonably have avoided. Defendant's conduct alleged is unfair
10 under all of these tests.

11 123. As a direct and proximate result of Defendant's unfair practices, Plaintiff and
12 California Subclass Members were injured and suffered damages, a loss of privacy, and loss of the
13 value of their personal information in an amount to be determined at trial.

14 124. Plaintiff seeks to enjoin further unfair acts or practices by Defendant, to obtain
15 restitution and disgorgement of all monies generated as a result of such practices, and for all other
16 relief allowed under California Business & Profession Code §17200.

17 **COUNT VI**
18 **Unlawful Practices**
19 **In Violation of the California Unfair Competition Law**
20 **Cal. Bus. & Prof. Code § 17200**

21 125. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

22 126. Plaintiff brings this claim individually and on behalf of the California Subclass.

23 127. At all relevant times there was in full force and effect the California Unfair
24 Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, *et seq.*, which prohibits, *inter alia*, "any
25 *unlawful*, unfair, or fraudulent business act or practice" and "unfair, deceptive, untrue, or misleading
26 advertising." Cal. Bus. & Prof. Code §17200 (emphasis added).

27 128. In the course of their business, Defendant repeatedly and regularly engaged in
28 unlawful acts or practices that imposed a serious harm on consumers, including Plaintiff and
California Subclass members.

1 129. Defendant's acts and practices are unlawful because Defendant violated, and
2 continues to violate:

- 3 (a) The Constitution of California, Article I, Section 1;
4 (b) The California Computer Data Access and Fraud Act;
5 (c) The California Invasion of Privacy Act; and
6 (d) Section 5 of the Federal Trade Commission Act, 15 U.S.C. §45.

7 130. As a direct and proximate result of Defendant's unlawful practices, Plaintiff and
8 California Subclass members were injured and suffered damages, a loss of privacy, and loss of value
9 of their personal information in an amount to be determined at trial.

10 131. Plaintiff seeks to enjoin further unlawful acts or practices by Defendant, to obtain
11 restitution and disgorgement of all monies generated as a result of such practices, and for all other
12 relief allowed under California Business & Professions Code §17200.

13 **COUNT VII**
14 **Unjust Enrichment or Restitution**

15 132. Plaintiff realleges and reincorporates by reference all paragraphs alleged above.

16 133. Plaintiff brings this claim individually and on behalf of the Class.

17 134. Plaintiff and members of the Class conferred a benefit on Defendant through the use
18 and dissemination of Plaintiff's and Class members' personal information, geolocation data, and
19 communications.

20 135. Defendant received and is in possession of Plaintiff's and Class members' personal
21 information, geolocation data, and communications, which Defendant used and disseminated for its
22 own monetary benefit.

23 136. It is unjust under the circumstances for Defendant to retain the benefit conferred by
24 Plaintiff and Class members without compensating them.

25 **REQUEST FOR RELIEF**

26 WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks
27 judgment against Defendant, as follows:
28

- 1 (a) For an order certifying the Class under Fed. R. Civ. P. 23 and naming
2 Plaintiff as representatives of the Class and the California Subclass and
3 Plaintiff’s attorneys as Class Counsel;
- 4 (b) For an order declaring the Defendant’s conduct violates the statutes
5 referenced herein;
- 6 (c) For an order finding in favor of Plaintiff, the Class, and the California
7 Subclass on all counts asserted herein;
- 8 (d) For compensatory, statutory, and punitive damages in amounts to be
9 determined by the Court and/or jury;
- 10 (e) For prejudgment interest on all amounts awarded;
- 11 (f) For an order of restitution and all other forms of equitable monetary relief;
- 12 (g) For an order awarding Plaintiff and the Class and California Subclass their
13 reasonable attorneys’ fees and expenses and costs of suit.

14 **JURY TRIAL DEMANDED**

15 Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any
16 and all issues in this action so triable of right.

17 Dated: January 26, 2024

BURSOR & FISHER, P.A.

18 By: /s/ L. Timothy Fisher
19 L. Timothy Fisher

20 L Timothy Fisher (State Bar No. 191626)
21 1990 North California Blvd., Suite 940
22 Walnut Creek, CA 94596
23 Telephone: (925) 300-4455
24 Facsimile: (925) 407-2700
25 E-mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.

26 Joseph I. Marchese (*pro hac vice* forthcoming)
27 Julian C. Diamond (*pro hac vice* forthcoming)
28 1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

Attorneys for Plaintiff

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Claims Digital Ad Platform InMarket Unlawfully Tracks, Sells Users' Location Data via 'Spyware'](#)
