Rafey Balabanian (SBN 315962)
rbalabanian@edelson.com
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 Classes

IN THE UNITED STATES DISTRICT COURT

FOR NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

NOAH BENDER, individually and on behalf of all others similarly situated, *Plaintiff*, v. TWILIO INC., a Delaware corporation, *Defendant*.	Case No.: **CLASS ACTION COMPLAINT FOR:** **(1) Violation of 18 U.S.C. § 2510, *et seq.*;** **(2) Violation of Cal. Penal Code § 502; and** **(3) Violation of the Cal. Penal Code § 631.** **AND DEMAND FOR JURY TRIAL**

Plaintiff Noah Bender ("Plaintiff" or "Bender") brings this Class Action Complaint and Demand for Jury Trial against Twilio Inc. ("Twilio" or "Defendant") for eavesdropping on consumers' sensitive in-app communications. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. Twilio is a data mining company that eavesdrops on consumers' sensitive in-app communications.

2. Twilio developed and disseminated a software development kit (or "SDK") called Segment that enables backdoor access to consumers' devices and opens a data collection pipeline directly from consumers to Twilio. Thousands of developers have embedded Twilio's Segment SDK into their mobile apps allowing them to siphon data from millions of consumers.

3. The data Twilio collects from unsuspecting consumers is incredibly sensitive. Twilio collects consumers' in-app search terms, search results, keystrokes, button presses, page views, and consumers' names and email addresses. This data reveals consumers' likes, interests, and information about other behavioral attributes. By way of example, Twilio collects real-time data from the Calm meditation app—intended to help with various mental health issues—that reveals whether an individual is dealing with anxiety, depression, or any other issue.

4. Armed with a wealth of data on the consumer, Twilio leverages its proprietary artificial intelligence to correlate data from various sources to compile a comprehensive digital dossier on each consumer. This dossier includes detailed insights and analytics, enabling the prediction of consumer behavior, such as the likelihood of making a purchase.

5. Plaintiff and the putative Class are consumers whose sensitive keystrokes and search terms (among other In-App Activities) have been intercepted from their devices while using mobile apps with the Segment SDK embedded. Plaintiff and the Class do not know—nor could they—that the apps they regularly use have embedded the Segment SDK and, as such, could not have consented to Twilio's data collection practices.

PARTIES

6. Plaintiff Noah Bender is a natural person and citizen of the State of California.

7. Defendant Twilio Inc. is a corporation organized and existing under the laws of Delaware with its principal place of business located at 101 Spear Street, Suite 500, San Francisco, California 94105.

JURISDICTION AND VENUE

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

9. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

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

DIVISIONAL ASSIGNMENT

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

COMMON FACTUAL ALLEGATIONS

Twilio Surreptitiously Collects Search Terms, Keystrokes, and In-App Activity from Millions of Mobile Devices

12. Twilio promises to collect and control customer data and give "unparalleled insight into the way customers interact across channels to create a single, unified view of the customer journey." Their entire business model depends on collecting sensitive information from consumers' devices and sharing it with data partners such as advertising networks and data warehouses, among others.

13. The secret to Twilio's data pipeline is the collection of what the industry calls "first-party data," or data collected directly from consumers. Twilio accomplishes this task by developing a SDK called Segment.

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

15. On information and belief, over 11,000 mobile app developers integrated the Segment SDK. These apps include, among others, shopping, productivity, gaming, and even mental health apps.

16. Twilio surreptitiously collects sensitive data from consumers through its SDK in real time. Twilio collects identity information such as the consumer's name and email address, mobile advertising IDs ("MAIDs"), the mobile app name, and device fingerprint data (which includes the consumer's device make and model, operating system version, and cell phone carrier name among other information).

17. Twilio also collects consumers' in-app activities in real time. Twilio collects in-app search terms entered by the consumer, keystrokes, search results, in-app choices such as button clicks and menu selections, and the pages requested by the consumer (collectively, the "In-App Activity").

18. Indeed, Twilio designed its SDK to intercept the content of electronic communications between the consumer and the mobile app. Consumers entering text into a field in a mobile app or pressing a button intend to send messages to, or otherwise communicate with, the mobile app. Similarly, a mobile app rendering search results or a web page also communicates with the consumer in response to his or her request. The Segment SDK collects, in real time, the messages and/or communications intended for the mobile app, such as search queries the consumer enters and sends to the mobile app service, as well as the content of forms they fill out.

19. In the case of the Calm meditation app, the Segment SDK collects incredibly sensitive consumer data. Calm aims to help consumers with their mental health issues like stress, anxiety, and depression. When logging into Calm, a consumer can select their current mood (*e.g.*, panicked or stressed) and utilize the search bar to find content related to the consumer's current state of mind. Unbeknownst to consumers, the Segment SDK collects all in-app selections such as

the current mood and the consumer’s search terms, in real time, including the consumer’s name and email address.

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

21. Consumers inputting text in an app or selecting buttons intend to communicate with the mobile app service. At no point does Twilio inform consumers that its SDK is collecting their In-App Activity, nor does it prompt consumers to grant Twilio permission to access or collect any data whatsoever.

22. In the case of Calm, consumers are not informed by Calm, Twilio, or anyone else that Twilio’s SDK is collecting their In-App Activity, nor are consumers prompted to grant Twilio permission to access or collect any data whatsoever.

23. On information and belief, a consumer would never know whether any given app has the Segment SDK third-party eavesdropping and tracking software embedded. The entire data collection process takes place surreptitiously without the consumer’s knowledge or consent.

24. Twilio’s interception of a consumer’s In-App Activity reveals information about the consumer’s interests, the apps they downloaded onto their phone, preferences, shopping histories, and even insight into their mental health.

Twilio Creates a Digital Dossier on Consumers

25. Twilio’s Segment SDK collects names and email addresses from consumers along with various identifiers such a MAIDs and device fingerprint data, making it easy to track a consumer across various websites, apps, and devices.

26. Indeed, Twilio admits that it uses the data it collects across various apps and websites to create a unified profile about the consumer. Twilio touts, “Segment’s industry-leading

customer profiles merge the *complete activity history* of each customer across web, mobile, and other digital touchpoints into a single, identity-resolved profile" (emphasis added).

27. This process of collecting and correlating consumer data into one profile is called identity resolution. Twilio describes the process as such:

> Identity Resolution, also known as ID Resolution, entity resolution, identity mapping, or record linkage, is the practice of creating a single customer profile for every customer by unifying different data sets pulled from a variety of locations, including CRM, marketing and support tools, SMS records, third party databases, and more. Data teams use Identity Resolution to connect real-world data concerning a single person from a variety of sources so that all customer data and behavior is in the same record.

28. Equipped with a wealth of knowledge about the consumer, Twilio places the consumer into an audience "segment" and applies its artificial intelligence algorithms to the consumer profile in a process called "Predictive Traits." The Predictive Traits algorithm allows Twilio to predict a consumer's "propensity . . . to make a purchase," "[p]redict a customer's future spend over the next 90 days," and even "[p]roactively identify customers who are likely to stop using [a] product" among other behavioral predictions.

29. To make matters worse, Twilio has created a platform that allows sharing of the data it harvested with even more unknown third parties. For example, Twilio created integrations to share consumer data with marketing and advertising platforms such as Facebook Ads, Google Ads, TikTok Ads, and Snapchat Ads.

FACTS SPECIFIC TO PLAINTIFF

30. Plaintiff Bender downloaded and used the Calm meditation app on his Android device within the last year.

31. The developers of the Calm mobile app embedded the Segment SDK into its mobile app allowing Defendant to intercept communications between Plaintiff and Calm such as Plaintiff's keystrokes, button presses, search terms he input into the Calm app, the results of his searches, page views, his name, email address, information about which app(s) he uses, device IDs, and fingerprint data.

32. Plaintiff did not (and could not) grant Defendant permission to collect any

information—especially not his In-App Activity in the Calm app—from his device whatsoever.

33. Neither Defendant nor Calm informed Plaintiff, or otherwise disclosed to Plaintiff, that the Segment SDK was embedded in the Calm app, or that if he used the Calm app, Defendant would collect his personally identifiable information and In-App Activity. Plaintiff did not consent to Defendant's collection.

CLASS ACTION ALLEGATIONS

34. **Class Definitions**: Plaintiff Noah Bender brings this proposed class action pursuant to Federal Rule of Civil Procedure 23(b)(2) and Rule 23(b)(3) on behalf of himself and a Class and Subclass (collectively, the "Classes") of others similarly situated, defined as follows:

> **Class**: All individuals who downloaded and used an app on their mobile device (1) with Twilio's Segment SDK embedded into the app and (2) that did not publicly disclose "Twilio" in any of the app's notices or disclosures.
>
> **California Subclass:** All California residents who downloaded and used an app on their mobile device (1) with Twilio's Segment SDK embedded into the app and (2) that did not publicly disclose "Twilio" in any of the app's notices or disclosures.

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

35. **Numerosity**: The exact number of Class members is unknown and not available to Plaintiff at this time, but it is clear that individual joinder is impracticable. On information and belief, Defendant has surreptitiously collected the In-App Activity of millions of consumers who fall into the definition of the Class and Subclass. Class members can be identified through Defendant's records.

36. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the putative Classes, and those questions predominate over

any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

(a) Whether Defendant intercepted the contents of communications from Plaintiff and the Classes;

(b) Whether Defendant accessed Plaintiff's and the Classes' computer systems;

(c) Whether Defendant made an unauthorized connection with Plaintiff's and the Classes' mobile devices; and

(d) Whether Defendant used or attempted to use any information obtained from Plaintiff's and the Classes' mobile devices.

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

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

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

fostered, and uniformity of decisions will be ensured.

40. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definitions" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violation of the Wiretap Act
18 U.S.C. § 2510, *et seq.*
(On behalf of Plaintiff and the Class)

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

42. The Wiretap Act generally prohibits the intentional "intercept[ion]" of "wire, oral, or electronic communication[s]." 18 U.S.C. § 2511(1)(a).

43. By designing the Segment SDK to contemporaneously and secretly collect In-App Activity—including the search terms, button presses, and other text input into mobile apps by Plaintiff and the Class members—Defendant Twilio intentionally intercepted and/or endeavored to intercept the contents of "electronic communication[s]" in violation of 18 U.S.C. § 2511(1)(a).

44. Plaintiff and the Class did not consent to Defendant's collection, interception, or use of the contents of their electronic communications. Nor could they—Defendant's collection of In-App Activity is entirely without Plaintiff's and the Class's knowledge. Indeed, when Plaintiff and the Class interacted with a mobile app that embedded the Segment SDK, Twilio did not announce its presence nor inform Plaintiff and the Class that it is collecting, intercepting, or using the content of the communications intended for the mobile app.

45. Furthermore, Defendant did not act as a mere extension of the mobile app used by Plaintiff and the Class because it used the intercepted communications for its own purposes. Defendant Twilio used Plaintiff's and the Class's In-App Activity to correlate data across various mobile apps to create a unified customer profile that included Plaintiff's and the Class members' In-App Activity and interests. Furthermore, Twilio used the collected In-App Activity data to make various behavioral predictions about Plaintiff and the Class.

46. Defendant never obtained any consent whatsoever from Plaintiff and the Class.

47. Plaintiff and the Class suffered harm as a result of Defendant's violations of the

Wiretap Act, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(c)(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Violation of the California Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502
(<u>On behalf of Plaintiff and the California Subclass</u>)

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

49. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act ("CDAFA") to "expand 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). In enacting the statute, the Legislature emphasized the need to protect individual privacy: "[The] Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals[.]" *Id.*

50. Plaintiff's and the California Subclass members' mobile devices are "computers" or "computer systems" within the meaning of Section 502(b) because they are devices capable of being used in conjunction with external files and perform functions such as logic, arithmetic, data storage and retrieval, and communication.

51. Defendant violated the following sections of Cal. Penal Code § 502(c):

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

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

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

52. Defendant "accessed" Plaintiff's and the California Subclass members' computers and/or computer systems because it gained entry to and/or caused output from their mobile devices to obtain Plaintiff's and the California Subclass members' In-App Activity.

53. Defendant was unjustly enriched with the data it obtained from Plaintiff and the California Subclass.

54. Plaintiff and the California Subclass now seek compensatory damages, injunctive relief, disgorgement of profits, other equitable relief, punitive damages, and attorneys' fees pursuant to Section 502(e)(1)–(2).

THIRD CAUSE OF ACTION
Violation of the California Wiretap Act
Cal. Penal Code § 631
(<u>On behalf of Plaintiff and the California Subclass</u>)

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

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

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

57. Defendant's Segment SDK intercepted Plaintiff's and California Subclass members' specific input events such as the content of their search terms, keystrokes, page views, button presses, and other choices on their mobile devices, including their affirmative actions (such as installing a mobile app on their device), and therefore constitute communications within the scope of the California Wiretap Act.

58. Defendant's Segment SDK made an unauthorized connection with Plaintiff's and the

California Subclass members' devices and obtained their sensitive information including their search terms, keystrokes, In-App Activity, names, email addresses, mobile device IDs, device fingerprint data, and information about the mobile app(s) they downloaded.

59. Plaintiff and the California Subclass did not consent to Defendant's collection or use of their communications. Nor could they—Defendant's collection of In-App Activity is entirely without Plaintiff's and the California Subclass's knowledge. Indeed, when Plaintiff and the California Subclass interacted with a mobile app that embedded the Segment SDK, Twilio did not announce its presence nor inform Plaintiff and the California Subclass that it is collecting or using the content of the communications intended for the mobile app.

60. Furthermore, Defendant did not act as a mere extension of the mobile app used by Plaintiff and the California Subclass because it used the intercepted communications for its own purposes. Defendant Twilio used Plaintiff's and the California Subclass's In-App Activity to correlate data across various mobile apps to create a unified customer profile that included the Plaintiff's and the California Subclass members' In-App Activity and interests. Furthermore, Twilio used the collected In-App Activity data to make various behavioral predictions about Plaintiff and the California Subclass.

61. Furthermore, Defendant attempted to and/or shared the data it wrongfully obtained from Plaintiff and the California Subclass to third parties including advertisers and other platforms.

62. Defendant never obtained any consent whatsoever from Plaintiff and the California Subclass.

63. Plaintiff and the California Subclass seek an injunction and damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Noah Bender individually and on behalf of the Classes, prays for the following relief:

(a) An order certifying the Class and California Subclass as defined above, appointing Noah Bender as the representative of the Class and California Subclass, and appointing his counsel as Class Counsel;

(b) An order declaring that Defendant's actions, as set out above violate the Wiretap Act, 18 U.S.C. § 2510; the California Comprehensive Computer Data Access and Fraud Act, Cal Penal Code § 501; and the California Wiretap Act, Cal. Penal Code § 631.

(c) An injunction requiring Defendant to cease all unlawful activities;

(d) An award of liquidated damages, disgorgement of profits, punitive damages, costs, and attorneys' fees; and

(e) Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully submitted,

NOAH BENDER, individually and on behalf of all others similarly situated,

Dated: August 8, 2024

By: /s/ Rafey S. Balabanian
One of Plaintiff's Attorneys

Rafey Balabanian (SBN 315962)
rbalabanian@edelson.com
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 Classes