

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 Classes*

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

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

16 *Plaintiff,*

17 v.

18 TWILIO INC., a Delaware corporation,

19 *Defendant.*

Case No.:

20 **CLASS ACTION COMPLAINT FOR:**

- 21 **(1) Violation of 18 U.S.C. § 2510, et**
seq.;
22 **(2) Violation of Cal. Penal Code § 502;**
and
23 **(3) Violation of the Cal. Penal Code §**
631.

24 **AND DEMAND FOR JURY TRIAL**

25 Plaintiff Noah Bender (“Plaintiff” or “Bender”) brings this Class Action Complaint and
26 Demand for Jury Trial against Twilio Inc. (“Twilio” or “Defendant”) for eavesdropping on
27 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
28 belief.

NATURE OF THE ACTION

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

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

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

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

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

PARTIES

23
24 6. Plaintiff Noah Bender is a natural person and citizen of the State of California.

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

JURISDICTION AND VENUE

1
2 8. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)
3 because (i) at least one member of the Class is a citizen of a different state than Defendant, (ii) the
4 amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and (iii) none of the
5 exceptions under that subsection apply to this action.

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

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

DIVISIONAL ASSIGNMENT

12
13 11. Pursuant to Civil Local Rule 3-2(c)–(d), this case should be assigned to the San
14 Francisco Division because a substantial part of the events or omission giving rise to the claim
15 occurred within the county of San Francisco.

COMMON FACTUAL ALLEGATIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 ***Twilio Creates a Digital Dossier on Consumers***

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

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

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

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

5 Identity Resolution, also known as ID Resolution, entity resolution, identity
6 mapping, or record linkage, is the practice of creating a single customer profile for
7 every customer by unifying different data sets pulled from a variety of locations,
8 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.

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

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

19 **FACTS SPECIFIC TO PLAINTIFF**

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

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

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

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

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

6 **CLASS ACTION ALLEGATIONS**

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

10 **Class:** All individuals who downloaded and used an app on their mobile device (1) with
11 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.

12 **California Subclass:** All California residents who downloaded and used an app on their
13 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.

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

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

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

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

- 3 (a) Whether Defendant intercepted the contents of communications from
4 Plaintiff and the Classes;
- 5 (b) Whether Defendant accessed Plaintiff's and the Classes' computer systems;
- 6 (c) Whether Defendant made an unauthorized connection with Plaintiff's and the
7 Classes' mobile devices; and
- 8 (d) Whether Defendant used or attempted to use any information obtained from
9 Plaintiff's and the Classes' mobile devices.

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

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

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

1 fostered, and uniformity of decisions will be ensured.

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

4
5 **FIRST CAUSE OF ACTION**
6 **Violation of the Wiretap Act**
7 **18 U.S.C. § 2510, et seq.**
8 **(On behalf of Plaintiff and the Class)**

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

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

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

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

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

28 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

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

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 California Subclass)**

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

10 49. 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 50. Plaintiff’s and the California Subclass members’ mobile devices are “computers” or
18 “computer systems” within the meaning of Section 502(b) because they are devices capable of
19 being used in conjunction with external files and perform functions such as logic, arithmetic, data
20 storage and retrieval, and communication.

21 51. Defendant violated the following sections of Cal. Penal Code § 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).

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

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

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

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

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

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

16 Any person [from using] any machine, instrument, or contrivance, or in
17 any other manner . . . [from making] any unauthorized connection,
18 whether physically, electrically, acoustically, inductively, or otherwise,
19 with any telegraph or telephone wire, line, cable, or instrument, including
20 the wire, line, cable, or instrument of any internal telephonic
21 communication system, or who willfully and without the consent of all
22 parties to the communication, or in any unauthorized manner, reads, or
23 attempts to read, or to learn the contents or meaning of any message,
24 report, or communication while the same is in transit or passing over any
25 wire, line, or cable, or is being sent from, or received at any place within
26 this state; or who uses, or attempts to use, in any manner, or for any
27 purpose, or to communicate in any way, any information so obtained, or
28 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

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

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

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

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

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

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

23 **PRAYER FOR RELIEF**

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

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

1 as Class Counsel;

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

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

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

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

9 **JURY DEMAND**

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

11 Respectfully submitted,

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

14 Dated: August 8, 2024

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

17 Rafey Balabanian (SBN 315962)
18 rbalabanian@edelson.com
19 Jared Lucky (SBN 354413)
20 jlucky@edelson.com
21 EDELSON PC
22 150 California Street, 18th Floor
23 San Francisco, California 94111
24 Tel: 415.212.9300
25 Fax: 415.373.9435

26 Schuyler Ufkes*
27 sufkes@edelson.com
28 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

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Privacy Lawsuits Allege Twilio, Verve, Amplitude Software Dev Kits Steal Consumers' Data](#)
