Eve-Lynn Rapp*
erapp@edelson.com
Nina Eisenberg (SBN – 305617)
neisenberg@edelson.com
EDELSON PC
123 Townsend Street,
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Class

**Pro hac vice* admission to be sought

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

PAMELA MORENO, individually and on behalf of all others similarly situated, *Plaintiff*, v. SAN FRANCISCO BAY AREA RAPID TRANSIT DISTRICT, a public entity, ELERTS CORP., a Delaware corporation, *Defendants*.	Case No. 17-cv-2911 **CLASS ACTION COMPLAINT FOR:** **(1) Violations of the Cellular Communications Interception Act;** **(2) Violations of the Consumers Legal Remedies Act;** **(3) Violations of Privacy Rights Pursuant to the California Constitution Article I, Section 1; and** **(4) Intrusion Upon Seclusion** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Pamela Moreno ("Plaintiff or "Moreno") brings this Class Action Complaint ("Complaint") against Defendants San Francisco Bay Area Rapid Transit District ("BART") and Elerts Corp, ("Elerts") (together, "Defendants") based on their clandestine collection of private cell phone identifiers. Plaintiff, for her Complaint, alleges as follows upon personal knowledge as to herself and her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. According to the Pew Research Center, 95% of Americans own a cellphone, with more than 77% owning a smartphone. Cellphone adoption and usage is so great that Americans "treat them like body appendages," carrying phones on their persons at all times.[1] Such ubiquity has brought about previously unheard of privacy issues, including the near constant ability for the location of cellular devices and their owners to be tracked.

2. This is particularly concerning when governmental agencies, such as law enforcement, track cellular phones and their owners, *en masse*. One method used by law enforcement departments across the country to track persons in that way is through the use of international mobile subscriber identity-catching devices, also known as "Stingray" devices. With these identity-catching devices, operators mimic legitimate cell towers, causing any cellphone in range to disclose their unique cellular identifying number but leaving persons caught in the identity-catching device scheme ignorant that they are being monitored.

3. The California Legislature was cognizant of the threat posed by governmental agencies' unchecked power to track a "phone's unique numeric identifier and its physical location."[2] The Legislature identified "major policy concerns" stemming from governmental tracking, including that it "raises important constitutional questions about dragnet-style 'general searches' and their prohibition by the Fourth Amendment … ."[3] To bring transparency to these "dragnet-style" devices, in 2015, the Legislature passed the Cellular Communications Interception Act, Cal. Gov't Code § 53166 (the "Act"), which requires governmental agencies to "implement a usage and privacy policy" that is conspicuously posted online, among other things.

4. Unfortunately, BART, a regional governmental agency, and Elerts, a private software developer that focuses on making safety and security reporting apps, have released a

---

[1] *Americans' cellphone use nearly constant | Pew Research Center*, http://www.pewinternet.org/2015/08/26/chapter-1-always-on-connectivity/ (last visited May 18, 2017).

[2] *Id.*

[3] *Id.*

mobile application masquerading as a transit app that secretly collects Californians' unique cellular numeric identifiers and physical locations. Through their BART Watch mobile application (the "BART Watch App" or "App") available for free download in the Google Play store, Defendants have convinced tens-of-thousands of Californians to download the app to keep up with transit alerts, report incidents (anonymously or not), and to call the BART police with a press of a button.

5. However, a detailed review of the BART Watch App reveals that Defendants have been using it to secretly collect Californians' unique mobile device identification numbers, including International Mobile Equipment Identity ("IMEI") numbers and to periodically track their precise locations. To be clear, unique numeric cellular identifiers like IMEIs are not normally collected by transit apps like the BART Watch App. Indeed, Google admonishes app developers to follow certain "tenets when working with Android identifiers," with the first being to **"#1: Avoid using hardware identifiers**" such as IMEI.[4]

6. But by collecting the device identification numbers, locations, and other personal information, described more below, Defendants have amassed a trove of data through the App. BART, or any of the agencies it shares resources with, now have the ability to match previous non-descript numerical identifiers with personally identifying information. Operators of Stingray devices would normally see only unique cellular identifiers without any other personally identifiable information associated (e.g., name or email) with the numbers. *See* Figure 1. But by collecting tens of thousands of IMEIs along with other identifying information, it is possible to *deanonymize* that data. *See* Figure 2.

* * *

[4] *Best Practices for Unique Identifiers | Android Developers*, https://developer.android.com/training/articles/user-data-ids.html (last visited May 18, 2017.) (emphasis in original).

Suspend Results

Time	Provider	Band	Carrier	Color Code	Event Type	Subscribe...	TMSI	IMSI	IMEI	RSSI	SQE
9:10:49 AM	Nextel Wireless	800 MHz	0x37F	8	Location Update		B5E0633F	31601000...	00170014...	-84	20
9:07:50 AM	Nextel Wireless	800 MHz	0x37F	8	Location Update		B5913A54	31601000...	00170014...	-9[illegible]	19
9:06:25 AM	Nextel Wireless	800 MHz	0x37F	8	Location Update		B5DE8D20	31601002...	00170324...	-8[illegible]	21

Registration

(**Figure 1**, showing actual sample Stingray data with IMEIs circled in red.)

lastname	firstname	email	IMEI
Doe	Jane	janedoe@sample.com	354[redacted]
Doe	Jon	jondoe@sample.com	001700143409524

(**Figure 2**, showing demonstrative data constructed from information collected by Defendants.)

7. Defendants' implementation of its unique cellular numeric identifier catching device disguised as a transit app has been done without any of the protections provided by the Act and remains unchecked. Accordingly, this putative class action seeks (1) to stop Defendants' collection of devices' unique numeric cellular identifiers and physical locations, (2) to compel Defendants to purge their records of all device unique numeric cellular identifiers and physical locations already collected, (3) to compel Defendants to inform Plaintiff and the putative Class the identities of all parties who received access to collected devices' unique numeric cellular identifier and physical locations, (4) statutory damages, (5) nominal and punitive damages, and (6) attorneys' fees.

PARTIES

8. Plaintiff Pamela Moreno is a natural person and resident and citizen of the State of California.

9. Defendant San Francisco Bay Area Rapid Transit District is a California public entity operating under the laws of the State of California with its headquarters located at 300 Lakeside Drive, Oakland, CA 94612-3534. BART conducts business throughout this District.

10. Defendant Elerts Corp., is a corporation existing under the laws of Massachusetts, with its headquarters and principal place of business located at 1132 Main Street, Weymouth, Massachusetts 02190. Elerts conducts business throughout this District, the State of California, and the United States.

JURISDICTION AND VENUE

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

12. This Court has personal jurisdiction over Defendant BART because it is headquartered in California, conducts business in California, and because the unlawful events giving rise to this lawsuit occurred in California.

13. This Court has personal jurisdiction over Defendant Elerts because it conducts business in California. Specifically, Defendant Elerts contracted with BART for the design, development, and distribution of the App that targets California residents (especially those in the San Francisco Bay area). And, the causes of action in this case arose out of the App.

14. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred in, were directed to, and/or emanated from this District. 28 U.S.C. § 1391(b).

INTRADISTRICT ASSIGNMENT

15. Pursuant to Civil Local Rule 3-2(d), this case has been assigned to the Oakland Division.

FACTUAL BACKGROUND

I. An Overview of the Government's Surveillance Technology.

16. In March 2014, ABC10 of Sacramento reported on "9 California law enforcement agencies [that are] connected to cellphone spying technology."[5] ABC10 requested information from numerous California law enforcement agencies regarding their use of "Stingray" devices, which "is a device law enforcement uses to track people and collect real time data from every cellphone within a certain radius." ABC10 reported that in 2012, the Bay Area Urban Area Shield Initiative

[5] *9 Calif. law enforcement agencies connected to cellphone spying technology | ABC10.com*, http://www.abc10.com/news/investigations/watchdog/9-calif-law-enforcement-agencies-connected-to-cellphone-spying-technology/277656425 (last visited May 18, 2017).

provided grant money for Bay Area police "to ensure we have the ability to cover all of the Bay Area in deploying cellphone tracking technology in any region of the Bay Area at a moment's notice."

17. Following ABC10's report, many other newspapers and organizations reported on the widespread use of Stingrays across the country.[6]

18. Thereafter, the California legislature introduced a bill to limit the secret deployment of Stingrays and similar technology throughout the State. According to the Legislative Counsel's Digest, the bill was written to "require every local agency that operates cellular communications interception technology, as defined, to maintain reasonable operational, administrative, technical, and physical safeguards to protect information gathered through use of the technology from unauthorized access, destruction, use, modification, or disclosure and implement a usage and privacy policy, as specified, to ensure that the collection, use, maintenance, sharing, and dissemination of information gathered through use of the technology complies with applicable law and is consistent with respect for an individual's privacy and civil liberties."[7]

19. The California Legislature was particularly concerned about the government's use of communications interception technologies to "collect a variety of data about 'caught' cell phones, particularly the phone's unique numeric identifier and its physical location."[8] The mass collection

---

[6] *Stingrays, IMSI catchers: How local law enforcement uses an invasive surveillance tool.*, http://www.slate.com/articles/technology/future_tense/2014/11/stingrays_imsi_catchers_how_local_law_enforcement_uses_an_invasive_surveillance.html (last visited May 18, 2017); *Evidence of 'stingray' phone surveillance by police mounts in Chicago - CSMonitor.com*, http://www.csmonitor.com/World/Passcode/2014/1222/Evidence-of-stingray-phone-surveillance-by-police-mounts-in-Chicago (last visited May 18, 2017); *The Feds Are Now Using 'Stingrays' in Planes to Spy on Our Phone Calls | WIRED*, https://www.wired.com/2014/11/feds-motherfng-stingrays-motherfng-planes/ (last visited May 18, 2017); *LYE: Short-circuiting 'stingray' surveillance of cellphones - Washington Times*, http://www.washingtontimes.com/news/2014/jul/18/lye-short-circuiting-stingray-surveillance/ (last visited May 18, 2017); *'StingRay': Records Show Secret Cellphone Surveillance by Calif. Cops - NBC News*, http://www.nbcnews.com/tech/security/stingray-records-show-secret-cellphone-surveillance-calif-cops-n52181 (last visited May 18, 2017).

[7] *Bill Text: CA SB741 | 2015-2016 | Regular Session | Chaptered | LegiScan*, https://legiscan.com/CA/text/SB741/2015 (last visited May 18, 2017).

[8] *Id.*

of phones' unique numeric identifiers and physical location presented "major policy concerns" because such collection "can affect all mobile users in the vicinity of the device, not just individuals under investigation. This raises important constitutional questions about dragnet-style 'general searches' and their prohibition by the Fourth Amendment, as well as practical problems with service disruption for the public."[9]

20. While the Government might obtain a proper warrant to listen to the content of communications intercepted by the Stingray, the device also picks up bystanders' phones (e.g., the bystanders are "caught" in the dragnet). Normally, Stingray operators would only see numeric cellular identifiers, such as IMEIs, of all of those "caught" bystanders and would not be able to identify the owner of the cellular device. Figure 3 shows the user interface of a Stingray device and reveals the "caught" cellular identifiers, circled in red.

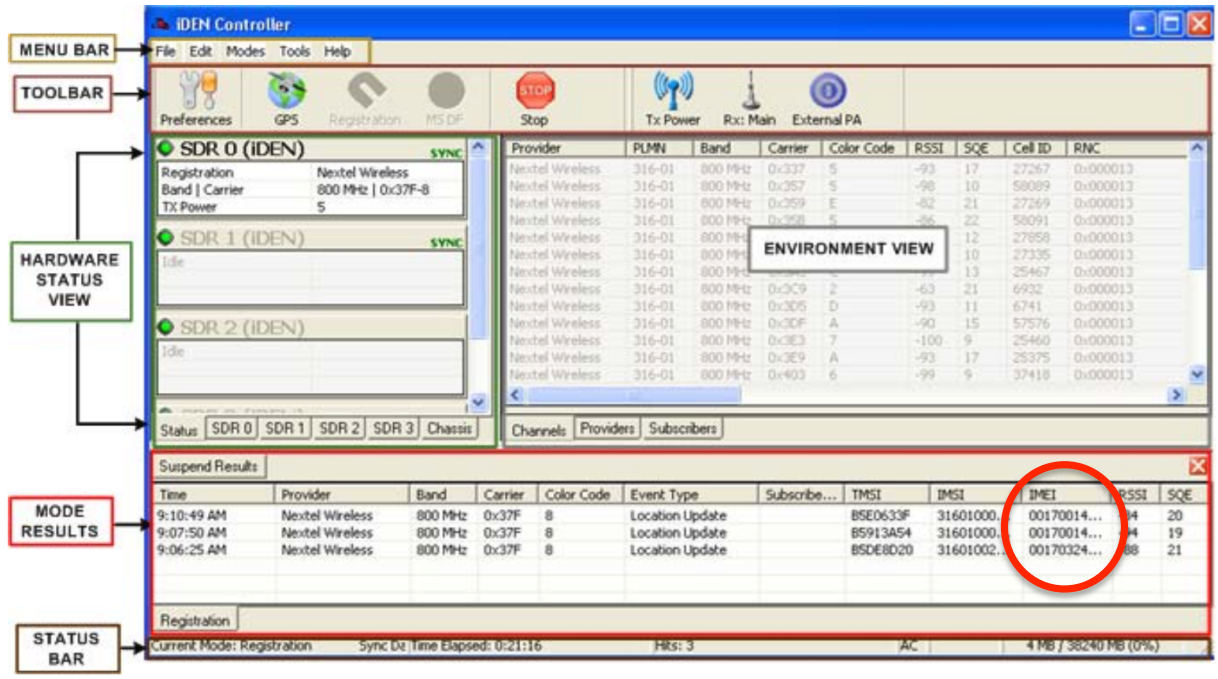


Figure 1-4. Main Screen Layout

(**Figure 3.**)

21. But if the government was able to obtain a database of IMEIs linked with persons' identities, it could, in real time, identify exactly who is "caught" in their Stingray net. *See* Figures 1

[9] *Id.*

and 2. Through the BART Watch App, Defendants have been secretly amassing tens of thousands cellular identifiers linked to personally identifiable information.

II. Defendants Partner To Develop and Distribute the BART Watch App.

22. BART is a governmental agency tasked with providing transportation across the Bay Area. BART operates across Alameda, Contra Costa, San Francisco, and San Mateo counties, providing transportation to over 120 million passengers a year. To protect passengers and property, BART employs almost 300 in its BART Police department which works closely with neighboring police departments, such as the San Francisco Police Department and the Oakland Police Department.

23. In 2014, BART, through its BART Police department, partnered with Elerts to develop and launch the BART Watch App for Android and iOS smartphones. Defendant BART has paid Elerts approximately $300,000 for the development of the BART Watch App.[10] In a press release, the Elerts CEO stated that "riders need an easy way to send a report to police. Our app provides San Francisco's transit riders with a quick and discreet option to alert security personnel about safety or security concerns."[11]

24. Defendants kept with the message of "discreet" interactivity in its marketing in the Google Play store:

> The BART Watch App offers the public a quick and discreet method for reporting suspicious activity directly to BART Police. The app can send pictures, text messages, and locations of suspicious people or activities. From the home screen, users have two easy options for contacting BART Police:
>
> * The "Report a Problem" button allows users to send text or photos directly to BART Police. To ensure discretion, the camera flash is automatically disabled when photos are taken through the app. When reporting an issue, users can select locations and report categories to assist BART Police. Riders can also send reports anonymously if they chose.

---

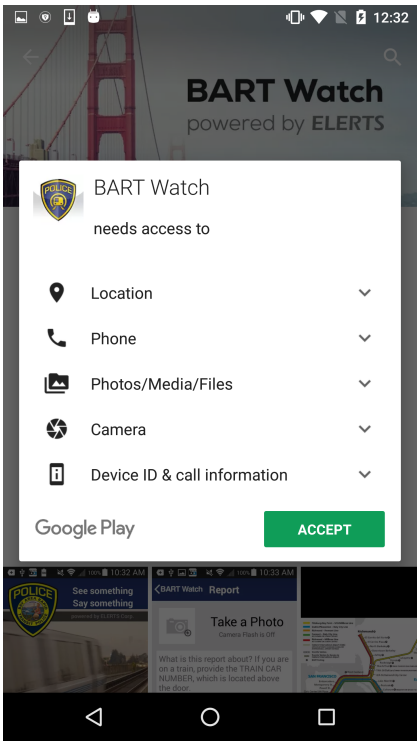
[10] *03-13-14 Minutes.pdf*, https://www.bart.gov/sites/default/files/docs/minutes/03-13-14%20Minutes.pdf (last visited May 18, 2017); *Microsoft Word - FY17 PBM Final.docx*, https://www.bart.gov/sites/default/files/docs/FY17%20Budget%20Pamphlet%20Final.pdf (last visited May 18, 2017).

[11] *ELERTS empowers riders of San Francisco BART system with "See Something, Say Something" smartphone app - ELERTS Corp.*, http://elerts.com/elerts-empowers-riders-san-francisco-bart-system-see-something-say-something-smartphone-app/ (last visited May 18, 2017).

> * The "Call BART Police" button will connect customers directly to BART Police.
>
> The application is designed for BART. If you send a report in an area without cellular connectivity, it will be stored and sent when connectivity returns. The system is also designed to send text messages before pictures so that BART Police can get app reports as quickly as possible.

25. The BART Watch App has been popular with Bay Area transit riders, with between 10,000 and 50,000 people downloading the App from the Google Play store alone.

26. When transit users first download the App, the Google Play store informs the users that the App requires access to certain phone functionality to operate. *See* Figure 4. For instance, the Google Play Store states that the App needs access to "Location," "Phone," "Photos/Media/Files," "Camera," and "Device ID & call information," permissions directly related to the advertised features of the App (e.g., calling police, taking photos to send to BART Police, and the ability to send location with a report).

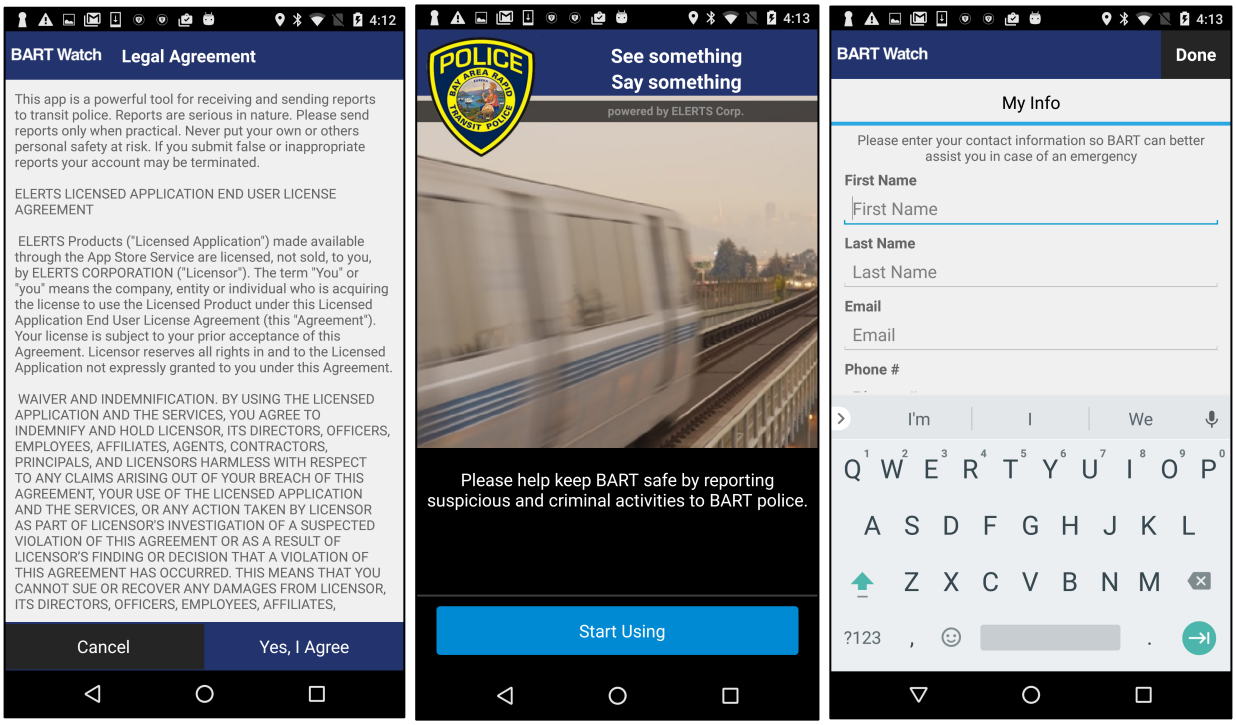


(**Figure 4.**)

27. After pressing the "ACCEPT" button, the App downloads to the transit users' smartphone. When the user opens the App for the first time, Defendants programmed the App to require transit users' assent to a "Legal Agreement," further described as the Licensed Application

End User License Agreement ("EULA.") *See* Figure 5, a true and accurate copy of the EULA is attached as Exhibit A.

28. After clicking on the "Yes, I Agree" button, Defendants programmed the App to show a splash screen telling the user to click on a "Start Using" button to proceed. Next, Defendants ask for "contact information so BART can better assist you in case of an emergency." *See* Figure 6. Although users are not required to enter information here, Defendants obfuscate that fact by placing that disclosure at the bottom of the page (which is blocked by the keyboard). Defendants hid a "Privacy" link behind the keyboard as well.



(**Figures 5-7**, showing initial App setup screens.)

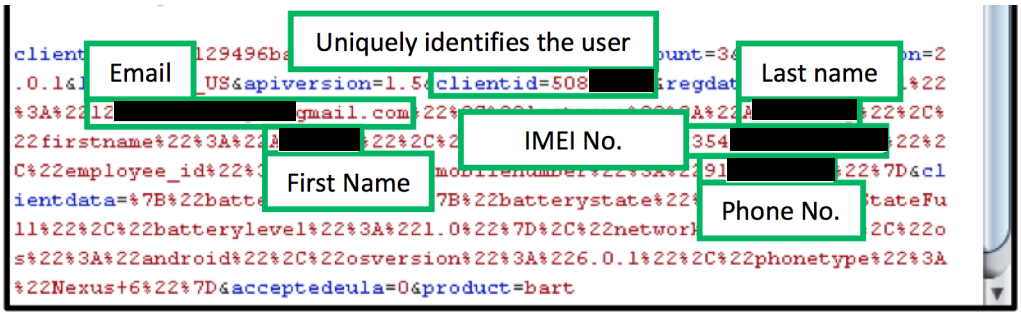
29. But while Defendants represent that the App is a "discreet" way of reporting issues and monitoring alerts (along with being able to report anonymously), Defendants actually programmed the App to secretly collect transit users' unique cellular identifiers, periodically monitor users' locations, and track the identities of anonymous reporters.

III. Defendants Secretly Collect Tens of Thousands of Residents' IMEIs and Precise Locations.

30. A forensic review of the App and how it communicates with Defendants' servers reveals that the BART Watch App was programmed to operate just as the communications

interception technologies the California Legislature has warned of. Indeed, the BART Watch App is designed to "collect a variety of data about 'caught' cell phones, particularly the phone's unique numeric identifier and its physical location."[12]

31. To start, reviewing the traffic sent to Defendants during initial setup of the App shows that when a user provides the optional contact information, it is sent with their cellular phones' unique numeric identifier. In the example shown in Figure 8, below, Defendants have accessed and then stored the phones' unique IMEI number and have caused the IMEI to be sent to their servers:



(**Figure 8.**)

32. In addition, Defendants create and transmit a unique "clientid" that is then associated with the contact information. Defendants also collect seemingly benign information, including such as "batterystate" and "batterylevel." *See* Figure 8. To data miners and others, this data is not benign. Rather, this exact type of information acts as "fingerprint" that can uniquely identify persons and "is being used to track [consumers] online."[13]

33. Even when transit users do not provide the optional contact information, Defendants still programmed the BART Watch App to create a unique "clientid," collect the cellular phone's unique identifier, and transit that information along with the other tracking data:

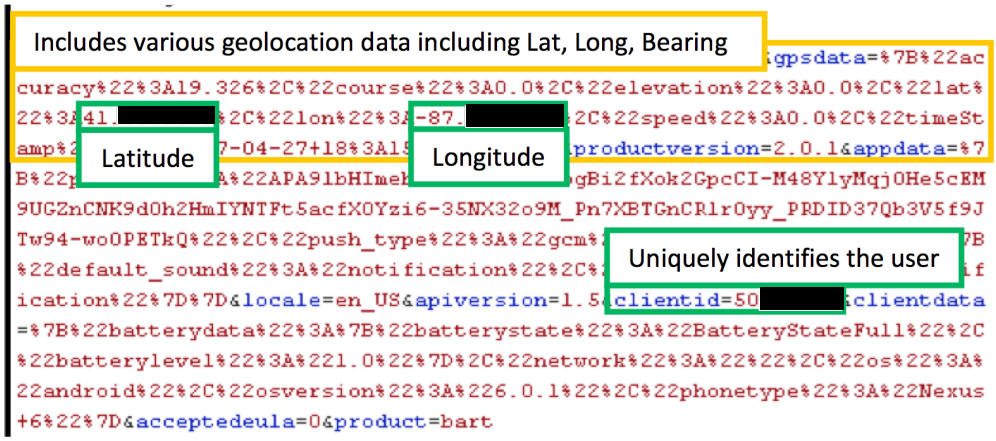
---

[12] *Bill Text: CA SB741 | 2015-2016 | Regular Session | Chaptered | LegiScan*, https://legiscan.com/CA/text/SB741/2015 (last visited May 18, 2017).

[13] *Your battery status is being used to track you online | Technology | The Guardian*, https://www.theguardian.com/technology/2016/aug/02/battery-status-indicators-tracking-online (last visited May 18, 2017.)

(**Figure 9.**)

34. After collecting the IMEI and tracking information during initial setup (along with any optional contact information Defendants acquired), Defendants also programmed the App to periodically transmit each transit user's clientid and precise location information to their servers:

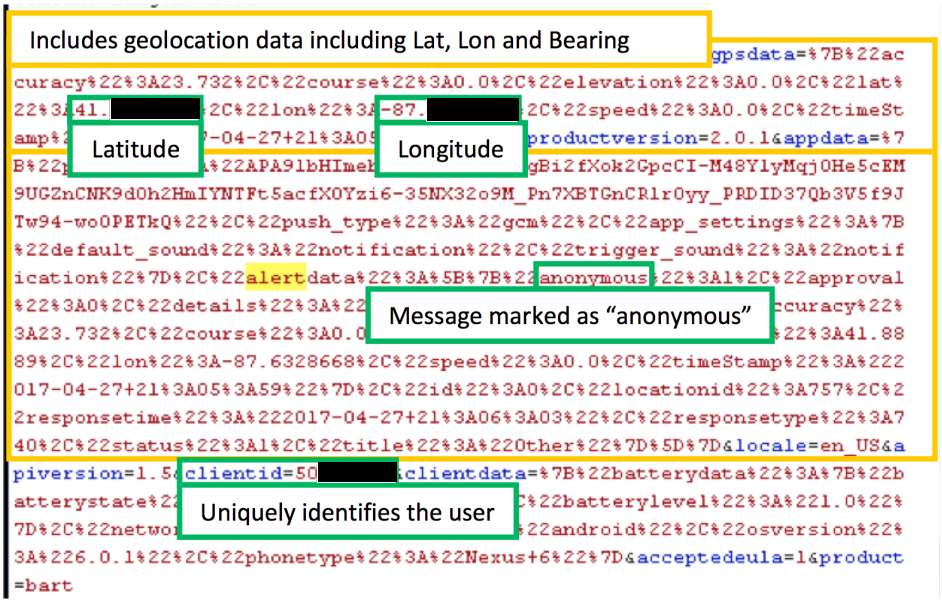


(**Figure 10**, showing periodic transmission of identifying information)

35. As Figure 10 shows, Defendants are collecting "gpsdata" and even such precise details as "course," "elevation," and "speed."

36. Worse, should a transit user submit an "anonymous" tip, Defendants still collect and transmit to their servers identifying information. As Figure 11 shows, Defendants include location information along with the "clientid" (i.e., which was originally created and transmitted to Defendants with the user's unique cellular identifier). As such, these reports are not anonymous at all.

* * *



(**Figure 11**, showing identifiable transmission resulting from "anonymous" report.)

37. Despite collecting a host of identifying, tracking, and sensitive data, Defendants do not obtain consent from transit users. While the Google Play store displays the App's request for permission to *access* location and certain other information, *see* Figure 4, Defendants do not request consent for their *collection and transmission* of that information.

38. Defendants understand the distinction between permission for the App's "access" to sensitive data and permission to collect and transmit that same data. In their EULA, Defendants state:

> In addition, when you use the Licensed Application to submit reports, and if you have enabled location services permission for the Licensed Application, the Licensed Application automatically includes your location in the Content transmitted to ELERTS and that location may be used by ELERTS consistent with the rights granted to ELERTS to use Content.

39. Although that clause is the only section of the EULA where Defendants reference the collection of location information, as demonstrated above, Defendants also periodically (and without user input) transmit transit users' locations to their servers. As such, Defendants further deceive transit users into thinking that their location is only sent to Defendants when the transit user takes the affirmative step of submitting a report.

40. Defendants' EULA is equally deceptive as to their cellular identifier collection scheme. Under a "Consent to Use of Data" clause, Defendants state that they collect unspecified

"technical information about your device, system and application software, and peripherals" for the purpose of "facilitate[ing] the provision of software updates, product support and other services to you (if any) related to the Licensed Application." Nowhere do Defendants mention that they actually create unique "clientids" and associate that with surreptitiously collected cellular identifiers (e.g., IMEIs).

41. Worse, Defendants have attempted to play "gotcha" with transit users by burying a purported "Privacy Policy" on the very last line of their EULA. Yet, Defendants placed a link to the "ELERTS Privacy" page immediately following a clause stating "This [EULA] Agreement constitutes the entire agreement" between the parties:

> j. This Agreement constitutes the entire agreement between you and ELERTS relating to the Licensed Application and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this Agreement will be binding unless in writing and signed by ELERTS. Any translation of this Agreement is done for local requirements and in the event of a dispute between the English and any non-English versions, the English version of this Agreement shall govern, to the extent not prohibited by local law in your jurisdiction.
>
> ELERTS Privacy: http://elerts.com/privacy/

(**Figure 12**.)

42. As such, the Privacy Policy is not incorporated with any contract with Plaintiff and members of the Class and is not enforceable. Indeed, Defendants know how to incorporate additional policies and terms into their EULA, which is why they drafted text (which wasn't included with the Privacy Policy) to do just that:

> By using this software in connection with an iTunes Store or a Google Play account, you agree to the latest iTunes Store or Google Play Terms and Conditions and Usage Rules, which you may access and review at in the case of the iTunes store at http://www.apple.com/legal/itunes/ww/ or Google Play at http://play.google.com/intl/en us/about/play-terms.html.

43. Nevertheless, and just as the Google Play permission screen and the EULA, Defendants' Privacy Policy lacks any specificity as to provide transit users notice of the scope of

Defendants' data collection practices. In the Privacy Policy, Defendants state that there are only three types of information they collect: "(i) information that you voluntarily provide to us (e.g. through a voluntary registration process); ii) reports that you submit using the Applications ("Reports"); and iii) other information that is derived through automated mechanisms."

44. When Defendants further explain the "automatically collected information," they obfuscate their actual collection practices. While the Privacy Policy states that Defendants "automatically receive your location when you use an Application to submit reports through that Application," Defendants do not disclose that they also programmed the App to automatically monitor transit users' precise locations on a periodic basis. *See* Figure 10.

45. Likewise, Defendants further conceal their data collection practices by making it seem that any data collected is incidental to app usage. Just as a person making a phone call might disclose their phone number when making a call (e.g., caller ID), Defendants' Privacy Policy describes that certain information is disclosed when transit users use the App: "When you use the Site or an Application, we may automatically receive and record information on our server logs from your browser or mobile device, including your location, IP address, browser type, operating information, mobile carrier, device and application IDs, cookie information, and the page you requested." As such, Defendants' Privacy Policy makes it appear as though their data collection is incidental to and an unavoidable part of using the App. However, Defendants do not disclose that they programmed the App to specifically target and collect unique cellular identifiers (e.g., IMEIs) and transmit the collected identifiers back to their servers. To be clear, Defendants' targeting and collection of unique cellular identifiers is not incidental to usage of any part of the App but reflects Defendants' intentional and out of the ordinary programming choice.

46. Defendants' undisclosed collection of cellular identifiers and locations *en masse* is precisely the practice the California Legislature sought to protect against when it passed the Cellular Communications Interception Act. As such, Plaintiff seeks (1) to stop Defendants' collection of devices' unique numeric cellular identifiers and physical locations, (2) to compel Defendants to purge their records of all device unique numeric cellular identifiers and physical locations already

collected, (3) to compel Defendants to inform Plaintiff and the putative Class the identities of all parties who received access to collected devices' unique numeric cellular identifier and physical locations, (4) statutory damages, (5) nominal and punitive damages, and (6) attorneys' fees.

FACTS RELATED TO PLAINTIFF PAMELA MORENO

47. Plaintiff downloaded the BART Watch App in 2016 onto her Samsung Galaxy S7 and used it regularly as a part of her commute.

48. At the time Plaintiff downloaded and used the App for the first time, she was not aware that the App was designed to (and actually did) collect her smartphone's unique numeric cellular identifier and physical location and then transmit that information to Defendants.

49. Had Defendants requested to collect that information and transmit it to Defendants' servers, Plaintiff would have declined.

50. In addition, Plaintiff would not have downloaded the App had she known that Defendants would be collecting smartphone's unique numeric cellular identifier and physical location.

CLASS ALLEGATIONS

51. **Class Definition**: Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of herself and a Class of similarly situated individuals, defined as follows:

> **Class:** All individuals who downloaded and opened the BART Watch App and who had their smartphone's unique numeric cellular identifier collected by Defendants.

Excluded from the Class is: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current, former, purported, and alleged employees, officers, and directors; (3) counsel for Plaintiff and Defendants; (4) persons who properly execute and file a timely request for exclusion from the Class; (5) the legal representatives, successors, or assigns of any such excluded persons; and (6) all persons who have previously had claims similar to those alleged herein finally adjudicated or who have released their claims against Defendants.

52. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this

time, but it is clear that individual joinder is impracticable. Defendants have listened in on thousands of consumers who fall into the Class definition. Ultimately, the Class members will be easily identified through Defendants' records.

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

a) whether Defendants' BART Watch App is cellular communications interception technology;

b) whether Defendants obtained consent to collect Plaintiffs' and the Class's unique numeric cellular identifiers and physical locations;

c) whether Defendants' conduct violated Cal. Gov't Code § 53166;

d) whether Defendants' conduct violates Consumers Legal Remedies Act Cal. Civ. Code §§ 1750, *et seq.*;

e) whether Defendants' conduct violates Plaintiff's and the Class's privacy rights under California Constitution article I, section 1;

f) whether Defendants' actions constitute intrusion upon seclusion; and

g) whether Plaintiff and the Class members are entitled to equitable relief as well as actual and/or statutory damages resulting from Defendants' conduct.

54. **Typicality**: Plaintiff's claims are typical of the claims of all the other Class members. Plaintiff and the Class members sustained substantially similar damages as a result of Defendants' uniform wrongful conduct, based upon the same interactions that were made uniformly with Plaintiff and the public.

55. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the other Class members. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the Class members and have the financial resources to do so. Neither Plaintiff nor her counsel has any interest adverse to those of the other Class members.

56. **Policies Generally Applicable to the Class**: Defendants have acted and failed to act on grounds generally applicable to Plaintiff and the other Class members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class.

57. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for individual Class members to obtain effective relief from Defendants' misconduct. Even if Class members could sustain such individual litigation, it would still 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, economies of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered and uniformity of decisions ensured.

58. Plaintiff reserves the right to revise the Class Definitions and Class Allegations based on further investigation, including facts learned in discovery.

FIRST CAUSE OF ACTION
Violation of the Cellular Communications Interception Act
Cal. Gov't Code § 53166
(On Behalf of Plaintiff and the Class)

59. Plaintiff incorporates by reference the foregoing allegations.

60. Defendants' BART Watch App is a cellular communications interception technology as defined by Cal. Gov't Code § 53166(a)(1) because it is a device that intercepts calling information and operates similar to an international mobile subscriber identity catcher.

61. As described throughout this Complaint, Defendants programmed the BART Watch App to collect Plaintiff's and the Class's unique numeric cellular identifiers and locations.

62. Defendants have violated the Act in at least the following ways:

(i) Cal. Gov't Code § 53166(b)(1) by not implementing reasonable security

procedures and practices before operating the BART Watch App;

(ii) Cal. Gov't Code § 53166(b)(2) by not implementing and conspicuously posting a usage and privacy policy with the required information under the Act; and

(iii) Cal. Gov't Code § 53166(c) by not having the BART Watch App and usage and privacy policy adopted by its legislative body at a public meeting.

63. Plaintiff and members of the Class have been harmed by Defendants' violation of the Act because their unique numeric cellular identifiers and locations have been collected by and transmitted to Defendants without their consent and without the protections provided by the Act.

64. Plaintiff seeks (1) actual damages, but not less than liquidated damages in the amount of two thousand five hundred dollars ($2,500); punitive damages, reasonable attorneys' fees and other litigation costs, and other preliminary and equitable relief as the Court determines to be appropriate, including a injunction prohibiting Defendants from continuing to collect unique numeric cellular identifiers and locations without disclosure and to destroy records related to any unique numeric cellular identifiers and locations they have already collected.

65. Plaintiff seeks damages against only Defendant Elerts at this time.

SECOND CAUSE OF ACTION
Violation of the Consumers Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq.*
Against All Defendants
For Injunctive Relief Only
(On Behalf of Plaintiff and the Class)

66. Plaintiff incorporates by reference the foregoing allegations.

67. As described throughout, Defendants programmed their BART Watch App to collect and transmit unique cellular numeric identifiers and locations to their servers without Plaintiff's and members of the Class's consent.

68. The Consumers Legal Remedies Act ("CLRA") applies to Defendants' actions and conduct as described herein because it extends to transactions that are intended to result, or which have resulted, in the sale of goods or services to consumers.

69. Defendant is a "person" as defined by Cal. Civ. Code § 1761(c).

70. Plaintiff and each member of the Class are "consumers" as defined by Cal. Civ. Code § 1761(a).

71. Defendants' BART Watch App is a "good" within the meaning of Cal. Civ. Code § 1761(a).

72. As described herein, Defendant has engaged in deceptive practices, unlawful methods of competition, and/or unfair acts as defined by Cal. Civ. Code §§ 1750 *et seq.*, to the detriment of Plaintiff and the Class.

73. Defendant, acting with knowledge, intentionally and unlawfully brought harm upon Plaintiff and the Class by programming their BART Watch App to collect and transmit unique cellular numeric identifiers and locations to their servers without disclose to Plaintiff and members of the Class.

74. Specifically, Defendant violated Cal. Civ. Code § 1750 in at least the following respects:

a) In violation of § 1770(5), by representing that the BART Watch App had characteristics, ingredients, uses, benefits, or quantities which it did not have (e.g., that it offered a discrete method of issuing a report);

b) In violation of § 1770(7), by representing that the BART Watch App was of a particular standard, quality, or grade of which it was not (e.g., that it would only collect data and locations in limited circumstances); and

c) In violation of § 1770(9), by advertising the BART Watch App with the intent not to sell its goods as advertised (e.g., that it offered a discreet method of issuing a report and that it would only collect data and locations in limited circumstances).

75. Defendants' unfair or deceptive acts or practices were capable of deceiving a substantial portion of the purchasing public.

76. Defendants knew that they were unable or unwilling to manufacture, distribute, and sell the BART Watch App that followed its privacy representations. Specifically, Defendant

possessed technical materials and documentation and would have known that it programmed the App to periodically report on transit users' locations and to collect and transmit transit users' unique cellular numeric identifiers.

77. Once Defendants made specific public representations regarding the specifications of the BART Watch App, Defendants were under a duty to Plaintiff and the Class to disclose their inability or unwillingness to design and distribute the App as represented:

i. Defendants were in a superior position to know the true state of facts about the specifications of the BART Watch App;

ii. Plaintiff and the Class could not reasonably have been expected to learn or discover that Defendants did not design the BART Watch App with the advertised privacy representations;

iii. Plaintiff and the Class could not have reasonably expected that Defendants were omitting material terms regarding their privacy practices (that the App collects and transmits to them transit users' unique cellular numeric identifiers and locations);

iv. Defendant knew that Plaintiff and the Class members could not reasonably have been expected to learn or discover that the BART Watch App collects and transmits to them transit users' unique cellular numeric identifiers and locations; and

v. Defendant knew, and in fact intended, that Plaintiff and the Class members would rely on Defendant's representations regarding their privacy practices (or omissions of their actual practices) in choosing whether or not to download and run the BART Watch App.

78. In failing to disclose their inability or unwillingness to design, manufacture, and distribute the BART Watch App with the advertised privacy protections along with their failing to disclose their actual data collection practices, Defendants have knowingly and intentionally concealed material facts and breached their duty not to do so.

79. The facts concealed or not disclosed by Defendant to Plaintiff and the Class, including that the BART Watch App collects and transmits to them transit users' unique cellular

numeric identifiers and locations, are material in that a reasonable consumer would have considered them to be important in deciding whether or not to download and run the BART Watch App.

80. Plaintiff and the Class reasonably expect their unique cellular numeric identifiers and locations to be private unless they provide consent to share that information. Plaintiff's and Class members' expectations were reasonable under the circumstances.

81. That the BART Watch App collects and transmits to Defendants transit users' unique cellular numeric identifiers and locations is a material fact that should have been disclosed to Plaintiff and members of the Class.

82. Plaintiff and members of the Class relied on the representations made by Defendants about the BART Watch App when downloading and running the BART Watch App.

83. Defendants' false representations about the BART Watch App were acts likely to mislead Plaintiff and the members of the Class acting reasonably under the circumstances.

84. Through the misrepresentations and omissions detailed herein, Defendant wrongfully induced Plaintiff and the other members of the Class to purchase the BART Watch App when they otherwise would not have downloaded and used the BART Watch App.

85. As a direct and proximate result of Defendants' violation of Cal. Civ. Code §§ 1750, *et seq.*, Plaintiff and each Class member have suffered harm in the form of wear and tear on their smartphones, consuming the battery life of their smartphones, and diminishing their use, enjoyment, and utility of their devices.

86. Plaintiff and members of the Class request an injunction prohibiting Defendants from continuing to collect unique numeric cellular identifiers and locations without disclosure and to destroy records related to any unique numeric cellular identifiers and locations they have already collected.

87. Under Cal. Civ. Code § 1780(a) and (b), Plaintiff, individually and on behalf of the Class, seeks an injunction requiring Defendant to cease and desist the illegal conduct alleged in this Complaint, and all other appropriate remedies for its violations of the CLRA. For the sake of clarity, Plaintiff explicitly disclaims any claim for damages under the CLRA at this time.

THIRD CAUSE OF ACTION
Violation of Privacy Rights
California Constitution article I, section 1
Against All Defendants
(On Behalf of Plaintiff and the Class)

88. Plaintiff incorporates by reference the foregoing allegations.

89. The California Constitution protects citizens against unwanted access to data by electronic and covert means, in violation of the law and social norms. And Plaintiff and members of the Class have a specific, legally protected privacy interest in preventing government agencies (and the private companies helping them) from collecting without consent their unique cellular numeric identifiers and locations.

90. By programming their BART Watch App to collect and transmit unique cellular numeric identifiers and locations to their servers without disclose to Plaintiff and members of the Class, Defendant have accessed data by electronic and covert means, in violation of the law and social norms.

91. As described throughout the complaint, Defendants' data collection practices are abnormal in the transit app industry and run contrary to California norms. The California Legislature, the California press, and Californians are all concerned by governmental agencies that secretly collect unique cellular numeric identifiers and device locations.

92. Plaintiff and members of the Class have interests in precluding the dissemination or misuse of sensitive and confidential information. The California Legislature has recognized the interest Californians have in preventing the unauthorized collection of their unique cellular numeric identifiers and locations by governmental agencies through its passage of the Cellular Communications Interception Act.

93. Plaintiff and members of the Class have interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference. Specifically, Plaintiff and members of the Class have interests in providing or declining consent to corporations and governmental agencies seeking to track their unique cellular numeric identifiers and locations. By collecting Plaintiff's and the Class's unique cellular numeric identifiers and locations without first requesting consent, Defendants have frustrated Plaintiff's and the Class's

interest.

94. Plaintiff and members of the Class have reasonable expectations of privacy under the circumstances. Defendants offer the BART Watch App for free download in the Google Play Store and have disguised their data collection practices. As such, Plaintiff and members of the Class did not know that Defendants were collecting their unique cellular numeric identifiers and locations and transmitting the collected data back to Defendants' servers, and therefore could not consent to Defendants' practices.

95. Defendants secret collection and transmission of unique cellular numeric identifiers and locations constitute a serious invasion of Plaintiff's and the Class's privacy interests. Defendants' actions are sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.

96. Defendants understand that their data collection practices do not conform to social norms (and industry norms) which is why they have attempted to obfuscate their secret collection of unique cellular numeric identifiers and locations through a vague EULA and unenforceable Privacy Policy.

97. Plaintiff seeks an injunction against both Defendants prohibiting Defendants from continuing to collect unique numeric cellular identifiers and locations without disclosure and to destroy records related to any unique numeric cellular identifiers and locations they have already collected.

98. Plaintiff seeks damages against only Defendant Elerts at this time.

FOURTH CAUSE OF ACTION
Intrusion Upon Seclusion
Against All Defendants
(On Behalf of Plaintiff and the Class)

99. Plaintiff incorporates by reference the foregoing allegations.

100. Defendants intentionally intruded into a place, conversation, or matter as to which Plaintiff and members of the Class have a reasonable expectation of privacy.

101. By programming their BART Watch App to collect and transmit unique cellular numeric identifiers to their servers, Defendant have obtained unwanted access to data by electronic

and covert means, in violation of the law and social norms.

102. As described throughout the complaint, Defendants' data collection practices are abnormal in the transit app industry and run contrary to California norms. The California Legislature, the California press, and Californians are all concerned by governmental agencies that secretly collect unique cellular numeric identifiers and device locations.

103. Defendants' intrusion occurred in a manner highly offensive to a reasonable person. Defendants do not disclose their data collection practices and have attempted to disguise their secret collection of unique cellular numeric identifiers and locations through a vague EULA and unenforceable Privacy Policy.

104. Plaintiff seeks an injunction against both Defendants prohibiting Defendants from continuing to collect unique numeric cellular identifiers and locations without disclosure and to destroy records related to any unique numeric cellular identifiers and locations they have already collected.

105. Plaintiff seeks damages against only Defendant Elerts at this time.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Pamela Moreno, on behalf of herself and the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Pamela Moreno as representative of the Class, and appointing her counsel as Class Counsel;

B. Declaring that Defendants' actions, as described herein, violate the Cellular Communications Interception Act, the Consumers Legal Remedies Act, and California Constitution Article 1, Section 1, and constitute intrusion upon seclusion;

C. Awarding actual damages, but not less than liquidated damages in the amount of two thousand five hundred dollars;

D. Awarding punitive damages as appropriate;

E. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the

Class members, including, *inter alia*, an order prohibiting Defendants from collecting and storing unique numeric cellular identifiers and locations;

F. Awarding Plaintiff and the members of the Class their reasonable litigation expenses and attorneys' fees;

G. Awarding Plaintiff and the members of the Class pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

PAMELA MORENO, individually and on behalf of all others similarly situated,

Dated: May 22, 2017

By: /s/ Nina Eisenberg
One of Plaintiff's Attorneys

Eve-Lynn Rapp*
erapp@edelson.com
Nina Eisenberg (SBN – 305617)
neisenberg@edelson.com
EDELSON PC
123 Townsend Street
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Class

**Pro hac vice* admission to be sought