AUDET & PARTNERS, LLP
MARK BURTON (SBN 154061)
Email: mburton@audetlaw.com
MICHAEL McSHANE (SBN 127944)
Email: mmcshane@audetlaw.com
221 Main Street, Suite 1460
San Francisco, CA 94105
(415) 568-2555 Telephone
(415) 568-2556 Facsimile

ZIMMERMAN REED, LLP
CALEB MARKER (SBN 269721)
Email: caleb.marker@zimmreed.com
HANNAH P. BELKNAP (SBN 294155)
Email: hannah.belknap@zimmreed.com
2381 Rosecrans Ave., Suite 328
Manhattan Beach, CA 90245
(877) 500-8780 Telephone
(877) 500-8781 Facsimile

Attorneys for Plaintiff and the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MICHAEL GONZALES, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

UBER TECHNOLOGIES, INC., a Delaware corporation, UBER USA, LLC, a Delaware limited liability company, RAISER-CA, a Delaware limited liability company, and DOES 1-10, inclusive,

Defendants.

CASE NO.: 3:17-CV-02264

COMPLAINT (CLASS ACTION)

1. Violation of the ECPA (18 U.S.C. § 2511)
2. Violation of the CIPA (Penal Code § 630 *et seq.*)
3. Violation of California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200 *et seq.*)
4. Invasion of Privacy

(Jury Trial Demanded)

Plaintiff Michael Gonzales, individually and on behalf of all similarly situated persons, by and through the undersigned attorneys alleges the following.

NATURE OF THE ACTION

1. Plaintiff, Michael Gonzales, brings this action on his own behalf and as a class action for the benefit of a Class consisting of Lyft drivers whose electronic communications and whereabouts were intercepted, accessed, monitored, and/or transmitted by Defendants.

2. Plaintiff and the Class seek injunctive relief and damages caused by Defendants' unlawful invasion of privacy and interception of electronic communications and images in violation of the Federal Wiretap Act as amended by the Electronic Communications Privacy Act (hereinafter referred to as the "Wiretap Act" or the "Electronic Communications Privacy Act"), the California Invasion of Privacy Act ("CIPA"), and common law damages for invasion of privacy.

3. Plaintiffs and the members of the Class were employed as drivers for Lyft during the time period that Uber deployed spyware code-named "Hell."

4. Defendants intentionally developed spyware that allowed it to gain unauthorized access to computer systems operated by its competitor, Lyft, and pose as Lyft customers. Using Hell, Uber employees, contractors, and/or agents were able to access the location of up to eight Lyft drivers (e.g., Class members) at one time and obtain their unique Lyft ID. Each Lyft ID Is unique, akin to a social security number, which allowed Uber to track Lyft drivers' locations over time.

5. Upon information and belief, Uber repeated this process millions of times using its sophisticated Hell spyware's digital capabilities from 2014 through 2016.

6. Upon information and belief, Uber used the location data to determine which Lyft drivers also worked for Uber by combining the data obtained from Hell with its internal records of the historical location data of its own drivers. In lay terms, Uber was looking for overlap between the location data so that it could target drivers working for both platforms in order to improve the Uber platform and harm the Lyft platform. Uber accomplished this by incentivizing drivers working on both platforms to work primarily for Uber, thereby reducing the supply of Lyft drivers which resulted in increased wait times for Lyft customers and diminished earnings for Lyft drivers.

7. Courts have confirmed that tracking the GPS of an individual "chills associational and expressive freedoms." *United States v. Jones*, 565 U.S. 400, 413, 132 S. Ct. 945, 954, 181 L. Ed. 2d 911 (2012) (Sotomayer, J., concurring). "…GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.*, quoting *United States v. Cuevas–Perez*, 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring).

8. The same principles identified by the Supreme Court in *Jones* apply to the GPS tracking by an opaque entity that operates either as its targets' employer or their employer's competitor.

9. Uber has never publicly acknowledged the use of its Hell spyware but did not deny its existence when asked to respond to news reports.

10. Despite Uber's knowledge of which Lyft drivers had their Personal Information compromised by the Hell spyware, Uber has never provided notice to any Class Members.

11. Defendants have yet to provide any notice to these individuals that their private information was breached and remains compromised.

THE PARTIES, JURISDICTION AND VENUE

12. Plaintiff and the Class bring this action pursuant to §§ 2511 and 2520 of title 18 of the United States Code also known as the Electronic Communication Privacy Act ("ECPA") or Wiretap Act.

13. This Court has original jurisdiction of Plaintiffs' and the Class' federal law claims pursuant to 28 U.S.C. §§ 1331 and 1337.

14. This Court also has jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367, as those claims are so related to the claims in the action within the original jurisdiction that they form part of the same case or controversy.

15. Plaintiff Michael Gonzales ("Plaintiff") is an adult resident of California.

16. Plaintiff Gonzales was employed as a driver for Lyft from 2012 until approximately November 2014.

17. During the time period Plaintiff Gonzales worked for Lyft, he drove passengers in the San Francisco Bay Area, including, but not limited to, the counties of San Francisco, San Jose, and San Mateo.

18. At no time has Plaintiff Gonzales ever worked for any Defendant or any subsidiaries or affiliates of any Defendant.

19. At no time has Plaintiff Gonzales ever executed any contract or arbitration agreement with any Defendant.

20. Defendant Uber Technologies, Inc. is a Delaware corporation and maintains a principal place of business at 1455 Market Street, Fourth Floor, San Francisco, California 94103.

21. Defendant Uber USA, LLC is a Delaware limited liability company and maintains a principal place of business at 1455 Market Street, Fourth Floor, San Francisco, California 94103.

22. Defendant Rasier-CA, LLC is a Delaware limited liability company and maintains a principal place of business at 1455 Market Street, Fourth Floor, San Francisco, California 94103.

23. Together, Defendants Uber Technologies, Inc., Uber USA, LLC, and Rasier-CA, LLC are referred to jointly as the “Defendants” or “Uber.”

24. “[A]ccording to financial information Uber shared with Bloomberg,”[1] Uber booked more than $20 billion in revenues and $6.5 billion in revenue.

25. Uber operates in more than 75 countries and relies heavily on foreign funding, including more than $3.5 billion from the Saudi Arabian sovereign wealth fund.[2]

26. Lyft operates as Uber’s main competitor in the United States.

27. Plaintiff does not know the true names and capacities of the defendants sued herein as Does 1 through 10 (“Doe Defendants”), inclusive, and therefore sues said Doe Defendants by fictitious names. Plaintiffs are informed and believe and based thereon allege that each of the Doe Defendants is contractually, strictly, negligently, intentionally, vicariously liable and/or otherwise legally

[1] https://www.bloomberg.com/news/articles/2017-04-14/embattled-uber-reports-strong-sales-growth-as-losses-continue

[2] https://www.bloomberg.com/news/articles/2016-06-03/uber-s-deal-with-saudi-arabia-hasn-t-gone-down-well-with-saudi-women

responsible in some manner for the acts and omissions described herein. Plaintiff will amend this Complaint to set forth the true names and capacities of each Doe Defendant when the same are ascertained.

28. Plaintiff is informed and believe and based thereon allege that Uber and Doe Defendants 1 through 10, inclusive, and each of them, are and at all material times have been, the agents, servants or employees of each other, purporting to act within the scope of said agency, service or employment in performing the acts and omitting to act as alleged herein. Each of the Defendants named herein are believed to, and are alleged to, have been acting in concert with, as employee, agent, co-conspirator or member of a joint venture of, each of the other Defendants, and are therefore alleged to be jointly and severally liable for the claims set forth herein, except as otherwise alleged.

29. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391 because Defendants resides in this District, conduct substantial business in this District and the Plaintiff worked as a Lyft driver in this District.

30. Venue is also proper in this District because the Defendants received, managed, accessed, intercepted and transmitted communications collected in this District.

31. In connection with the acts and conduct complained of below, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including the internet, or made such use possible.

CLASS ACTION ALLEGATIONS

32. Plaintiff brings this action against Defendants pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and all other persons similarly situated. Plaintiff seeks to represent the following classes:

The National Class

> All individuals in the United States who (1) worked as drivers for Lyft, (2) while not working for Uber, and (3) whose private information and whereabouts was obtained by Uber by accessing computer systems operated or used by Lyft and the Class (the "Class").

The California CIPA Class Claim

> All individuals who (1) worked as drivers for Lyft, (2) while not working for Uber, and (3) whose private information and whereabouts was obtained by Uber by accessing computer systems operated or used by Lyft and the Class (the "California Class Claim").

33. The "Class Period" dates back four years (or the length of the longest applicable statute of limitations for any claim asserted) and continues through the present and the date of judgment.

34. Excluded from the Class are: (a) any officers, directors or employees of Uber or Lyft; (b) any judge assigned to hear this case (or spouse or family member of any assigned judge); (c) any employee of the Court; and (d) any juror selected to hear this case. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

35. All requirements for class certification in Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2) or 23(b)(3) (or any other applicable state or federal rule of civil procedure) are satisfied with respect to the Class and the Class. Plaintiff and the respective Class Members were injured by Uber's deployment and use of its Hell spyware for many years. Uber subjected Plaintiff and each Class Member to the same unfair, unlawful, and deceptive practices and harmed them in the same manner.

36. Numerosity: The proposed classes are so numerous that joinder of all members would be impracticable. According to public reports, more than 315,000 individuals have driven for Lyft in the United States and perhaps 60% of those individuals have also driven for Uber.[3] Thus, the number of Class Members in the National Class who never worked for Uber may number 126,000 or more. Common sense dictates that thousands of those individuals are California residents.

37. Ascertainability: The community of interest among Class members in the litigation is well defined and the proposed classes are ascertainable from objective criteria. If necessary to preserve the case as a class action, the court itself can redefine the Class. Both Uber and Lyft maintain highly

[3] https://www.theinformation.com/ubers-top-secret-hell-program-exploited-lyfts-vulnerability

detailed and accurate databases of their respective drivers and individual Class Members have access to accurate records that can confirm their membership in the proposed Class.

38. Plaintiff's claims are typical of the Class, as Plaintiff and all other Class Members were injured in exactly the same way - by the unauthorized collection, interception and/or transmission of their personal information and electronic communications, all through the Hell spyware.

39. Plaintiff will fairly and adequately represent the interests of the Class and have retained counsel competent and experienced in class action and complex litigation.

40. Plaintiff has no interests that are contrary to or in conflict with those of the Class.

41. A class action is superior to other available methods for the fair and efficient adjudication of this controversy under the acts described below. Given the nature of these claims, the expense and burden of individual litigation make it virtually impossible for the Class Members individually to seek redress for the unlawful conduct alleged.

42. Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

43. Common questions of law and fact exist as to all members of the Class and predominate over any questions effecting solely individual members of the Class. Among the questions of law and fact, common to the Class:

a. Whether Defendants' acts as alleged herein violated the ECPA;

b. Whether Defendants' acts as alleged herein violated the CIPA;

c. Whether Defendants' acts as alleged herein constituted invasions of Plaintiff's privacy; and

d. Whether Plaintiff and members of the Class are entitled to compensatory damages, as well as statutory and punitive damages pursuant to the ECPA.

44. Plaintiff brings this action under Rule 23(b)(2) because Defendants have acted or refused to act on grounds generally applicable to all members of the Class, thereby making final relief concerning the Class as a whole appropriate. In the absence of appropriate injunctive relief requiring Defendants to notify all Class Members that their private information has been breached, Class

Members will suffer irreparable harm. Defendants' uniform conduct towards Plaintiff and the other members of the Class makes certification under Rules 23(b)(2) appropriate.

45. Plaintiff also brings this action under Rule 23(b)(3) because common questions of law and fact identified herein predominate over questions of law and fact affecting individual members of the Class. Indeed, the predominant issues in this class are whether Defendants have violated the law by the unauthorized, inappropriate and undisclosed invasion of privacy, and by their remote interception and transmission of communications and information secretly obtained, and in the intentional unauthorized interception and use of electronic and computer communications and information. Certification under Rule 23(b)(3) is appropriate because:

e. by virtue of the secret nature of the Hell spyware described in this complaint, individual class members may not be aware that they have been wronged and are thus unable to prosecute individual claims or take appropriate steps to protect their private information;

f. concentration of the litigation concerning this matter in this Court is desirable;

g. the claims of the representative Plaintiffs are typical of the claims of the members of the purported class;

h. a failure of justice will result from the absence of a class action; and

i. the difficulties likely to be encountered in the management of this class action are not great.

SUBSTANTIVE ALLEGATIONS

46. Details of Uber's spyware code-named Hell emerged on or around April 12, 2017.

47. Prior to news reports on April 12, 2017, Uber actively concealed the existence and scope of its Hell spyware.

48. The Washington Post chronicled the history of Uber during 2017, thus far:

> March 3
>
> Reports surfaced that Uber had used a secret tool, known as Greyball, that allowed the company to circumvent government investigators in a years-long game of cat-and-mouse. The tool was designed to help Uber avoid abusive riders, but the company started using it to thwart regulators in places where the service was restricted or banned. Uber used Greyball to serve members of law enforcement a fake version of the app

> designed to prevent them from successfully hailing rides when investigating the company's practices. Uber also turned Greyball on cabdrivers to thwart them from using the Uber app to learn the whereabouts of Uber drivers. The revelation was a reminder of other covert actions Uber had taken to defeat its competition.
>
> * * *
>
> April 12
>
> According to a report by The Information, Uber operated a top-secret program known as "Hell," which sought to identify drivers for Uber competitor Lyft. The program not only helped Uber in locating Lyft drivers, potentially giving Uber a competitive advantage, the report said, but could also identify which Lyft drivers also drove for Uber. Those drivers would then be singled out for special driver-retention efforts, meaning that they were treated differently from Uber's most loyal workers. Legal analysts said the program could be viewed as an example of an "unfair business practice," which could land Uber in court.
>
> April 14
>
> California regulators said that Uber may be subject to more than $1 million in fines after the company repeatedly failed to take action against drivers that passengers said were driving drunk. Uber investigated only 13 percent of passenger reports about drunken driving, according to California's Public Utility Commission. Uber has promoted its ride-hailing service, in part, by arguing that it reduces drunken driving by keeping inebriated passengers from getting behind the steering wheel.

Brian Fung, *From #deleteUber to 'Hell': A short history of Uber's recent struggles*, THE WASHINGTON POST (April 18, 2017), available at http://wapo.st/2nSRGqF?tid=ss_tw .

49. Amir Efrati, writing for THE INFORMATION, described Uber's Hell spyware as follows:

> As the ride-sharing market was exploding in the U.S. between 2014 and the early part 2016, Uber had an advantage over Lyft that helped Uber maintain its lead, The Information has learned. Thanks to a secret software-based effort within Uber called "Hell," Uber could track how many Lyft drivers were available for new rides and where they were, according to a person who was involved in the program and a person who was briefed about it.
>
> More importantly, "Hell" showed Uber employees which of the tracked drivers were driving for both Lyft and Uber, helping Uber figure out how to lure those drivers away from its rival. That's a crucial edge in a business where finding enough people to drive is a constant battle.
>
> THE TAKEAWAY
>
> The revelation of a controversial Uber program aimed at hurting rival Lyft could further complicate CEO Travis Kalanick's attempt to lead Uber out of its deepening cultural and management crisis. It also opens up the company to potential legal claims.
>
> Only a small group of Uber employees, including top executives such as CEO Travis Kalanick, knew about the program, said the person who was involved in it. Not even Uber's then-powerful "general managers" who ran the business in individual cities were supposed to know about it.

The program, part of the company’s competitive intelligence, or “COIN,” group, was referred to as “Hell” because it paralleled Uber’s dashboard of Uber drivers and riders known as “God View,” or “Heaven.”

“Hell” was discontinued sometime in the early part of 2016, this person said. This person asked for anonymity because they aren’t authorized to discuss Uber’s internal matters. A spokesman for Uber said the company wouldn’t publicly discuss its internal processes. Lyft said in a statement: "We are in a competitive industry. However, if true, these allegations are very concerning."

Revelation of the program could open up Uber to possible civil legal claims by Lyft, according to lawyers from two law firms that have represented Uber on other matters. Such potential state and federal claims could include “breach of contract”; “unfair business practices”; misappropriation of trade secrets; and a civil violation of the federal Computer Fraud and Abuse Act because of the way Uber allegedly accessed information from Lyft. Such an action could give Lyft the ability to probe certain Uber business practices in court. Antitrust claims also are a possibility if Uber used Hell to help maintain its market power over Lyft—it generates between 70% to 85% of ride-hailing app revenue versus Lyft in key U.S. cities, according to third parties and people inside the companies—these lawyers said.

The public disclosure of Hell and Mr. Kalanick’s involvement with it also could make it harder for him to pull Uber out of a deepening cultural and management crisis that started in mid-February. Four of his 13 direct reports have resigned because of conflicts with Mr. Kalanick or because their past behavior was questioned. Mr. Kalanick, despite losing credibility with employees and executives throughout his company because of a variety of revelations, has said he is determined to continue as CEO, albeit with help from a COO he is trying to hire.

Spoofed Riders

Uber and Lyft have waged a war for market share in the U.S. since 2012, when Uber launched UberX, a lower-cost version of its ride-hailing service that let most anyone use their car to pick up Uber riders. UberX was similar to Lyft, which had launched a month earlier. Uber leveraged its early lead in riders, thanks to a high-end “black car” version of the service that began three years earlier, to capture market share against Lyft.

In 2014, Lyft expanded its operations from 20 cities to 65 cities, covering most major U.S. metro areas—places where Uber had already been operating for some time. Lyft’s market share was thus small but the company was able to take advantage of the demand for, and awareness of, ride-hailing that Uber had generated previous to Lyft’s entrance.

A key weapon in the war between the companies was getting enough drivers so that riders don’t have to wait long for a ride. Recruiting drivers through advertising and other marketing has been Uber’s top operating expense, judging by confidential financial statements 2015 seen by The Information. That expense easily could have reached $1 billion in 2016, assuming a steady rate of growth.

Hell started like this: Uber created fake Lyft rider accounts and used commonly available software to fool Lyft’s system into thinking those riders were in particular locations, according to the person. (That in and of itself is a violation of Lyft’s terms of service, which prohibits users from “impersonat[ing] any person or entity,” which Lyft riders must agree to when they open the app.)

The spoofed Lyft accounts made by Uber then could get information about as many as eight of the nearest available Lyft drivers who could accommodate a ride request. Uber made sure that in each city where it was competing with Lyft, the fake rider locations were organized in a grid-like format so that it could view the entire city.

In other words, Uber could see, nearly in real time, all of Lyft's drivers who were available for new rides—and where those drivers were located. That also allowed Uber to track the prices Lyft would offer to riders for certain trips, and how many cars were available to pick up riders at a particular time in one city or another.

Lyft's Flaw

But Uber executives realized there was a vulnerability in Lyft's system. The information about the nearby Lyft drivers included a special numbered ID, or token, that was tied to each individual driver. That ID remained consistent over time. So Uber could identify the same drivers again and again no matter where they were in a city. Thus, it learned some of those drivers' habits, such as what time of day or what days of the week they would run the Lyft app. (Uber constantly changes the IDs of its drivers for the Uber app so they can't be tracked in the same way, said the person involved with Hell.)

Here's the critical part of Hell: Because Uber tracked Lyft's drivers over time, it was able to figure out which of them were driving for Uber too, because it would be able to match the locations of its own drivers with those of Lyft. In many cities, more than 60% of Lyft's drivers also drive for Uber because they want to maximize their earnings. (As of a year ago, Lyft said it had about 315,000 drivers.) Uber thus had specific identities and contact information for the majority of Lyft's weekly or monthly active drivers in a particular place. "We achieved ground truth," said the person involved in the program.

Armed with data about when and where Lyft's drivers were operating, Uber aimed to sway them to work only for Uber instead, this person said. One way was to give them special financial bonuses for reaching a certain number of rides per week.

Uber employees involved with the Hell program passed along a list of drivers that should be targeted by the city general managers, who oversaw driver bonus budgets at that time.

Another goal of the program was to make sure Uber steered rides more reliably to Uber drivers who were also available on the Lyft network than to those who weren't, this person said. In other words, if there were several Uber drivers near an Uber rider but one of those drivers was also frequently available on the Lyft network, as seen by the Hell program, Uber's ride-dispatch team was supposed to "tip" that ride request to the driver who was "dual apping," or typically looking for riders through both the Lyft and Uber apps, sometimes by using two different smartphones at the same time.

The person involved in the program called it "privileged dispatch" and said Uber aimed to use that to squeeze Lyft's supply of drivers. This person didn't know how much the ride-dispatch team used data derived from Hell as part of its calculations. An Uber spokesman said the company does not give preference to "dual-apping" drivers.

"Hustle"

It's unclear if anyone at Uber quantified how helpful Hell was to its business overall, but the program got information about Lyft's network across the country, said the person who was involved with it. During meetings with the small group of people

> involved in Hell, Mr. Kalanick would often praise the team for the work they were doing and how well it fit into Uber's culture of "hustle" in order to win.
>
> While it's hard to estimate the potential impact of Hell on Lyft, even after the program was shut down, Uber could derive value from knowing which of its drivers were active drivers for Lyft generally, at least for a period of time. "The damage was done," this person said.
>
> Uber and Lyft have other ways of finding out which of their drivers might be driving for the competition. For instance, Lyft can see whether certain of its drivers—those who use Android-powered smartphones—also have the Uber app installed on their phone. (The Android operating system allows app developers to "scan" the phones to see what other apps are on them.) The iPhone is different. Apple stopped allowing app scanning on iPhones starting in mid-2015. But Hell gave Uber much more valuable data.
>
> Hell was overseen by several employees, including a product manager and data scientists who had special access to a room at Uber's headquarters in San Francisco, where the intel on Lyft's drivers was collected via computers that had the spoof accounts, this person said.
>
> Some at Uber might argue that some drivers benefited from Uber's surveillance of Lyft because they made more money when Uber decided to boost their bonuses or give them more rides. But the drivers who benefited most were those who showed less loyalty to Uber. Also, the destruction of Lyft would be bad for drivers in the long run. Lyft's presence in the market has ensured greater bonuses overall, though those may need to disappear if either company wants to make a profit. …

Amir Efrati, *Uber's Top Secret "Hell" Program Exploited Lyft's Vulnerability*, THE INFORMATION (April 12, 2017), available at https://www.theinformation.com/ubers-top-secret-hell-program-exploited-lyfts-vulnerability (attached hereto as Exhibit A).

50. Upon information and belief, all of the information and allegations contained in the article quoted in the preceding paragraph is true and accurate. The content of the article in the preceding paragraph and attached as Exhibit A is incorporated by reference herein.

51. From at least 2014 to 2016, Uber secretly deployed the Hell spyware and/or software on computer systems, including servers and smartphones, owned and operated by Lyft and Class Members.

52. As designed, Hell enabled Defendants to remotely and surreptitiously access, monitor, intercept, and/or transmit personal information as well as electronic communications and whereabouts.

53. Upon information and belief, Uber's Hell spyware enabled Uber to engage, and Defendants did in fact engage, in illegal, surreptitious, and unauthorized remote electronic surveillance, intrusion on Plaintiff and Class Members' privacy, seclusion, anonymity, whereabouts, and the interception of protected private communications.

54. Upon information and belief, Uber's Hell spyware was developed, written, manufactured, assembled, and utilized by Uber for the purpose of allowing Uber to remotely spy on Plaintiff and class members, as well as track, access, monitor, intercept and/or transmit electronic communications on Lyft and Class Members' computer systems.

55. Upon information and belief, Uber's Hell spyware was designed to be invisible or generally undetectable to Lyft, Class Members, and other end users of Lyft's computer systems.

56. Upon information and belief, Uber did engage in the conduct described in the preceding paragraphs.

57. Upon information and belief, Uber profited from the Hell spyware in a number of ways.

58. Upon information and belief, Uber directed more frequent and more profitable trips to Uber drivers that were determined to also work as Lyft drivers using Hell. This had the effect of making it more difficult for these drivers to accept work from the Lyft platform, encouraging the drivers to work primarily for Uber while reducing the effective supply of Lyft drivers available.

59. With the effective supply of Lyft drivers reduced, Lyft customers faced longer wait times. As a result, Lyft drivers may cancel the ride requested with Lyft and request a new ride from Uber to obtain a driver faster. Over time, this would have been very damaging to the Lyft market, harming drivers such as Plaintiff and absent Class Members.

CAUSES OF ACTION

COUNT I

(Violation of the ECPA, 18 U.S.C. § 2511, on behalf of the National Class)

60. Plaintiff incorporates all preceding and succeeding allegations by reference as if fully set forth herein.

61. Defendants have intentionally intercepted and/or procured to be intercepted Plaintiff's and Class Members' electronic communications without Plaintiffs' or the Class Members' knowledge, authorization, or consent in violation of 18 U.S.C. § 2511.

62. Defendants have also intentionally used and/or procured to be used a devise to intercept the above-referenced electronic communications.

63. An “electronic communication” is defined in § 2510(12) as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.

64. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally, collecting, gathering intercepting, endeavoring to intercept, transmit, procure, store any other person to intercept or endeavor to intercept Plaintiff’s and Class Members’ electronic communications.

65. Defendants violated 18 U.S.C. § 2511(1)(c) by intentionally collecting, transmitting, storing and disclosing, or endeavoring to disclose, to any other person, the contents of Plaintiff’s and Class Members’ electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiff’s and Class Members’ electronic communications.

66. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using or endeavoring to use, the contents of Plaintiffs’ and Class Members’ electronic communications, knowing or having reason to know that the information was obtained through the interception of private electronic communications.

67. Neither Plaintiff nor Class Members authorized or consented to Defendants’ interception of electronic communications.

68. Section 2520 of the ECPA provides for a private cause of action and allows for declaratory and equitable relief as appropriate and statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, and reasonable attorney's fees and costs.

<u>COUNT II</u>

(Violation of the CIPA, Penal Code § 630 *et seq.*, on behalf of the Class)

69. Plaintiff incorporates all preceding and succeeding allegations by reference as if fully set forth herein.

70. The California Invasion of Privacy Act (“CIPA”) was enacted in 1967 for the express purpose “to protect the right of privacy of the people of this state.” Penal Code § 630. The California Legislature declared that with the advent of new devices and technology used “for the purposes of eavesdropping upon private communications,” the resulting invasion of privacy from the “use of such

devices and techniques has created a serious threat to the free exercise of personal liabilities and cannot be tolerated in a free and civilized society."

71. Among other prohibitions, the California Invasion of Privacy Act prohibits using an electronic recording device to eavesdrop or record confidential communications between devices. Penal Code Section 632.

72. Among other prohibitions, the California Invasion of Privacy Act prohibits using an electronic tracking device to determine the location or movement of a person. Penal Code Section 637.7.

73. Any person who has been injured by a violation of the CIPA may bring an action against the person who committed the violation for the greater of the following amounts: (1) five thousand dollars ($5,000) per violation; (2) three times the amount of actual damages, if any, sustained by the plaintiff.

74. Further, any person may bring an action to enjoin and restrain any violation of California Invasion of Privacy Act. It is not a prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.

75. Defendants violated the California Invasion of Privacy Act, *inter alia*, when intercepting private communications between the Class and Lyft, including but not limited to, the driver's identification and pricing information, as well as tracking the locations of Class Members as described herein.

<u>COUNT III</u>

(Violation of the UCL)

76. Plaintiff incorporates all preceding and succeeding allegations by reference as if fully set forth herein.

77. Plaintiff brings this claim individually and on behalf of the Class against Defendants.

78. This cause of action is brought pursuant to California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* ("the UCL").

79. Defendants engaged in unlawful and unfair conduct under the UCL through its unlawful, unethical, and immoral use of its Hell spyware as described more fully herein.

80. Defendants' actions and practices constitute "unlawful" business practices in violation of the UCL because, among other things, they violate the ECPA as detailed in Plaintiff's first cause of action.

81. Defendants' actions and practices constitute "unlawful" business practices in violation of the UCL because, among other things, they violate the CIPA as detailed in Plaintiff's second cause of action.

82. Defendants' actions and practices constitute "unfair" business practices because Defendants' practices, as described throughout this complaint, offends established public policy and is immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers.

83. Defendants' actions and practices constitute "unfair" business practices because Defendants' practices, as described throughout this complaint, represent "conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition." *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 186, 973 P.2d 527, 543 (1999).

84. As a direct and proximate result of Defendants' violations, Plaintiff and members of the Class have suffered and continue to suffer injury in fact and lose money or property as a result of Defendant's conduct.

85. Plaintiff, on behalf of himself and the Class, seeks: (a) injunctive relief in the form of an order requiring Defendant to cease the acts of unfair competition alleged herein and purge all ill-gotten personal and private information from Defendants' computers and records; (b) restitution; (c) declaratory relief; and (d) attorney fees and costs pursuant to Cal. Code Civ. P. § 1021.5, *inter alia*.

COUNT IV

(Invasion of Privacy)

86. Plaintiff incorporates all of the proceeding paragraphs herein.

87. The California Constitution declares that:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

Cal. Const. art. I, § 1.

88. As described herein, Defendants engaged conduct that invaded Plaintiff's and Class Members' privacy interests, including, but not limited to, their private electronic communications and their whereabouts throughout the course of time.

89. The privacy interests invaded by Defendants through use of the Hell spyware involved both classes recognized in California: "(1) interests in precluding the dissemination or misuse of sensitive and confidential information (informational privacy"); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference (autonomy privacy)." *Hill v. National Collegiate Athletic Association*, 7 Cal. 4th 1, 35, 865 P.2d 633, 654 (1994).

90. Plaintiff and Class Members had a reasonable expectation of privacy as to the interests invaded.

91. Defendants' invasion of Plaintiff and Class Members' privacy interests was serious and sustained over several years.

92. Defendants' invasion of Plaintiff and Class Members' privacy interests caused Plaintiff and Class Members to suffer injury and damages.

93. The intentional and deliberate invasion of privacy as referenced herein constituted wanton, willful, and malicious conduct justifying an award of punitive damages against these Defendants.

PRAYER FOR RELIEF

Plaintiff, on behalf of himself and the Class, prays for relief as follows:

A. For an order certifying that the action may be maintained as a class action and appointing Plaintiffs and their undersigned counsel to represent the Class in this litigation;

B. For an order declaring that the acts and practices of Defendant constitute violations of the ECPA;

C. For an order declaring that the acts and practices of Defendant constitute violations of the CIPA;

D. For an order declaring that the acts and practices of Defendant constitute violations of Cal. Bus. & Prof. Code § 17200 *et seq.*;

E. For a permanent injunction enjoining Defendant from continuing to harm Plaintiff and members of the Class and the public, and violating California and federal law in the manners described above;

F. For restitution;

G. For actual and statutory damages pursuant to ECPA;

H. For actual and statutory damages pursuant to CIPA;

I. For nominal, compensatory, and punitive damages where appropriate;

J. For reasonable attorneys' fees and the costs of the suit; and

K. For all such other relief as this Court may deem just and proper and may be available at law or equity.

/ / /

/ / /

/ / /

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury of all claims so triable.

ZIMMERMAN REED, LLP

Dated: April 24, 2017 By: /s/ Caleb Marker

Caleb Marker
caleb.marker@zimmreed.com
Hannah P. Belknap
hannah.belknap@zimmreed.com
2381 Rosecrans Ave., Suite 328
Manhattan Beach, CA 90245
Tel. (877) 500-8780
Fax (877) 500-8781

Mark Burton
mburton@audetlaw.com
Michael McShane
mmcshane@audetlaw.com
AUDET & PARTNERS, LLP
221 Main Street, Suite 1460
San Francisco, CA 94105
Tel. (415) 568-2555
Fax (415) 568-2556

Counsel for Plaintiff and the Class