BURSOR & FISHER, P.A.
Joel D. Smith (SBN 244902)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: jsmith@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

E.S., a minor, individually and on behalf of all others similarly situated,

Plaintiff,

v.

LIFE360 INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff E.S., a minor (hereinafter "Plaintiff"), brings this action on behalf of himself and all others similarly situated against Defendant Life360 Inc. (hereinafter "Defendant" or "Life360"). Plaintiff makes the following allegations pursuant to the investigation of his counsel and are based upon information and belief, except as to the allegations specifically pertaining to himself, which are based on personal knowledge.

NATURE OF THE CASE

1. This case addresses the surreptitious, non-consensual, sale of millions of mobile device users' geolocation by Defendant. For years, Life360 has been a popular family safety app marketed as a great way for parents to track their children's movements using their cellphones. However, unbeknownst to Life360's users, the app has been selling data on childrens' and families' whereabouts to approximately a dozen data brokers who sell that data to virtually anyone who wants to buy it.

2. By selling data in this way, Defendant profits from the Plaintiff's and class members' data time and time again to countless third parties.

3. Defendant's undisclosed sale of Plaintiff and class members' data is not only unlawful but is also potentially dangerous, because it can provide malevolent actors with the tools needed to target particular members of society.

4. By selling this data without consent, Defendant has been unjustly enriched and has violated Plaintiff's privacy rights, state consumer protection and privacy statutes, and Section 5 of the FTC Act.

JURISDICTION AND VENUE

5. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2) because this is a class action in which at least one member of the class is a citizen of a state different from any Defendant, the amount in controversy exceeds $5 million, exclusive of interest and costs, and the proposed class contains more than 100 members.

6. This Court has personal jurisdiction over the Defendant because Defendant maintains its principal place of business in this District and because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

7. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District and because Defendant maintains its principal place of business in this District.

PARTIES

8. Plaintiff E.S. is a minor and a resident of Lawtey, Florida. Plaintiff's father downloaded the Life360 on or around July 2018. During that entire time, the app has tracked the geolocation of Plaintiff and his entire family.

9. Plaintiff's geolocation has been sold by Defendant to third parties. Defendant sold Plaintiff's location data until approximately January 2022.

10. Neither Plaintiff nor Plaintiff's parents consented to have Plaintiff's geolocation data sold to specific third parties for valuable consideration. If either Plaintiff or Plaintiff's parents had been aware that Defendant would sell their geolocation data to third parties, neither Plaintiff nor Plaintiff's parents would have used the Life360 App.

11. Plaintiff has not directly contracted with Defendant but to the extent that he is a party to any contract with Defendant, Plaintiff hereby disaffirms his contract with Defendant pursuant to Cal. Fam. Code § 6710 and equivalent statutes and legal rights nationwide.

12. Defendant Life360 Inc. is Delaware corporation with its principal place of business in San Francisco, California.

GENERAL BACKGROUND

13. Contrary to its reassurances to its users, Defendant tracks and stores users' locations and movements to amass a vast and comprehensive store of highly valuable geolocation data which it has and continues to commercially exploit.

14. Life360 has approximately 33 million users and is one of the largest sources of location data in the data broker industry.

15. When confronted with these allegations, the founder and CEO of Life360, Chris Hulls, admitted that Life360 sold the geolocation data of its users, claiming that, "We see data as an important part of our business model that allows us to keep the core Life360 services free for the

majority of our users, including features that have improved driver safety and saved numerous lives."

16. Data brokers that have purchased location data from Defendant include Safegraph, Arity, Cuebiq, and X-Mode.

17. A former X-Mode engineer has said the raw location data the company received from Life360 was among X-Mode's most valuable offerings due to the sheer volume and precision of the data, while a former Cuebiq employee stated that the company wouldn't be able to run its marketing campaigns without Life360's constant flow of location data.[1]

18. David Hull has admitted doing business with at least some of these data brokers, specifically stating X-Mode buys data from Life360 and that it is one of "approximately one dozen data partners."

19. In 2020, Life360 claimed that it implemented a policy prohibiting the selling or marketing of Life360's data to any government agencies to be used for a law enforcement purpose.

20. However, X-Mode and Safegraph are both known to sell data to law enforcement agencies and provide raw data feeds to government partners.

21. While Life360's data policy ostensibly applies to any companies that Life360's customers share data with, its CEO admitted that it has no control over how its customers use the data and lacks the ability to monitor the activities of purchasers of their location data.

22. Justin Sherman, a cyber policy fellow at the Duke Tech Policy Lab, has stated that Defendant's privacy policy would not give Life360's users an indication of how far their data can travel.

23. Additionally, Defendant's privacy policy indicated that information that is sold to third parties is shared in "a form that does not reasonably identify you directly."

24. But this is not true as Defendant fails to take necessary precautions to ensure that location histories cannot be traced back to individuals.

[1] https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.

25. Defendant does not properly make efforts to fuzz, hash, aggregate, or reduce the precision of the location data to preserve privacy.

26. Researchers have repeatedly demonstrated how location data of the type that Defendant sells, that has been "anonymized" can easily be connected to the people from whom it came.

27. This is by design, since if Defendant had taken the necessary precautions to properly anonymize the data, the data would be less valuable to third parties.

28. Instead of properly obfuscating the data, Defendant relies on its customers and data partners to voluntarily obfuscate the purchased data based on their specific applications.

29. Advertisers, government agencies, and investors are willing to spend hundreds of thousands of dollars for location data and the insights that can be derived from it.

30. Marketers use location data to target ads to people near businesses, while investors buy data to determine popularity based on foot traffic. Government agencies have bought location data to track movement patterns and in one case to support "Special Operations Forces mission requirements overseas."

31. This supposedly anonymized location data can have disastrous effects on the lives of Users. For example, In July of 2021, a high-ranking Catholic priest resigned after a Catholic news outlet outed him by using location data from the gay dating app Grindr linked to his device. The report claimed to show that the priest frequented gay bars.

32. Grindr, like other apps such as the Life360 app, that feed data into this industry, is required to ask for location permissions when a user first opens the app.

33. In Life360's case, because of how the app works, it asks for the broadest location permissions possible for functional purposes. Many apps that use location data allow users to grant access only while it's in use. Because Life360 is for tracking whereabouts in real time, the app asks for location data at all times—and does not function unless that permission is turned on. However, when Life360 obtains permission to track geolocation, it does not also ask for permission to sell that geolocation information to specific third parties for valuable consideration.

34. For many Life360 users, their data may be shared with the company's partners within 20 minutes of being recorded.

35. Many app-users look for data brokers' code in apps for signs of an app sending data off to third parties. However, Life360 collects its data directly from the app and provides it to data brokers through its own servers. This makes it especially difficult for Users to determine that Life360 sells location data to third parties since Apple's and Google's app stores have no way of detecting this transfer of location data to a third party.

36. In fact, Life360's sale of location data violates the terms of the Google App store, which has a policy against selling location data.

37. Selling location data has become more and more central to the Defendant's finances. In 2016, the company made $693,000 from selling data it collected. In 2020, the company made at least $16 million—nearly 20 percent of its revenue that year—from selling location data.

38. Life360 has also acquired companies that expand its tracking—and potentially its data-gathering capacity. In 2019, the company purchased ZenScreen, a family screen-time monitoring app. And in April, it purchased the wearable location device company Jiobit, aimed at tracking younger children, pets, and seniors, for $37 million.

39. Life360's reliance on its data partners to voluntarily obfuscate the data that Defendant sells them is not reasonable as many of these data partners have themselves faced controversy over how they handle data and privacy.

40. For example, X-Mode was banned from most app stores after it was discovered that the company was selling location data from Muslim prayer apps like Muslim Pro to U.S. government contractors associated with national security, raising concerns about unconstitutional government surveillance. Public records show that X-Mode received at least $423,000 from the U.S. Air Force and the Defense Intelligence Agency for location data between 2019 and 2020. The company also sold data on Americans in profiled sets, like people who were drivers or likely to shop at department stores.

41. Another data partner, SafeGraph openly sells location data on Amazon's data marketplace, including a $240,000 yearly subscription to data on people across the U.S. Safegraph has boasted of selling location data for purposes including marketing, real estate, investing, and city planning.

42. Oregon Senator Ron Wyden has flagged SafeGraph as a "data broker of concern."

A. Life360's Data Can Be Used to Identify People and Track Them to Sensitive Locations

43. Precise geolocation data, such as the data sold by Defendant, may be used to track consumers to sensitive locations, including places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, medical facilities, and welfare and homeless shelters.

44. By plotting the latitude and longitude coordinates including geolocation data using publicly available map programs, it is possible to identify which consumers' mobile devices visited reproductive health clinics. Further, because each set of coordinates is time-stamped, it is also possible to identify when a mobile device visited the location. Similar methods may be used to trace consumers' visits to other sensitive locations.

45. As described above, the location data provided by Defendant is easily de-anonymized.

46. Defendant employs no technical controls to prohibit its customers from identifying consumers or tracking them to sensitive locations. For example, it does not employ a blacklist that removes from its data set location signals around sensitive locations including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at-risk populations, and addiction recovery.

B. Life360's Practices Cause and Are Likely to Cause Substantial Injury to Consumers

47. As described above, the data sold by Defendant may be used to identify individual consumers and their visits to sensitive locations. The sale of such data poses an unwarranted

intrusion into the most private areas of consumers' lives and causes or is likely to cause substantial injury to consumers.

48. For example, the data may be used to identify consumers who have visited an abortion clinic and, as a result, may have had or contemplated having an abortion.

49. In fact, it is possible to identify a mobile device that visited a women's reproductive health clinic and trace that mobile device to a single-family residence. The data set also reveals that the same mobile device was at a particular location at least three evenings in the same week, suggesting the mobile device user's routine. The data may also be used to identify medical professionals who perform, or assist in the performance, of abortion services.

50. As another example, the data could be used to track consumers to places of worship, and thus reveal the religious beliefs and practices of consumers.

51. As another example, the data could be used to track consumers who visited a homeless shelter, domestic violence shelter, or other facilities directed to at-risk populations. This information could reveal the location of consumers who are escaping domestic violence or other crimes.

52. In addition, because Defendant's data allows its customers to track consumers over time, the data could be used to identify consumers' past conditions, such as homelessness.

53. As another example, the data could be used to track consumers who have visited addiction recovery centers. The data could show how long consumers stayed at the center and whether a consumer relapses and returns to a recovery center.

54. Identification of sensitive and private characteristics of consumers from the location data sold and offered by Defendant injures or is likely to injure consumers through exposure to stigma, discrimination, physical violence, emotional distress, and other harms.

55. These injuries are exacerbated by the fact that once Defendant sells the data, it lacks any meaningful controls over who accesses its location data feed.

56. The collection and use of consumer location data are opaque to consumers, who typically do not know who has purchased their location data or how it is being used. Indeed, once information is collected about consumers from their mobile devices, the information can be sold

multiple times to companies that consumers have never heard of and never interacted with. Consumers have no insight into how this data is used – they do not, for example, typically know or understand that the information collected about them can be used to track and map their past movements and that inferences about them and their behaviors will be drawn from this information. Consumers are therefore unable to take reasonable steps to avoid the above-described injuries.

57. The harms described above are not outweighed by countervailing benefits to consumers or competition.

C. August 2022 Federal Trade Commission Action Against Data Broker for The Sale of Geolocation Data

58. In August 2022, the Federal Trade Commission ("FTC") took action against a data broker, Kochava, that sells geolocation data without proper consent for allegations that are substantially similar to this complaint. *Federal Trade Commission v. Kochava, Inc.*, Case No. 2:22-cv-00377-BLW.

59. According to the FTC's complaint, the "Unfair Sale of Sensitive Data," as described above constitutes a violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair or deceptive acts or practices in or affecting commerce."

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

CLASS ALLEGATIONS

61. Plaintiff seeks to represent a class defined as all persons in the United States whose data, including but not limited to their geolocation data, was sold by Defendant without their consent (the "Class").

62. Plaintiff also seeks to represent a subclass defined as all Class members who reside in the State of Florida whose data, including but not limited to their geolocation data, was sold by Defendant without their consent (the "Florida Subclass")

63. Specifically excluded from the Class are Defendant, Defendant's officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint ventures, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or Defendant's officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

64. Plaintiff reserves the right to expand, limit, modify, or amend the class definition, including the addition of one or more subclasses, in connection with his motion for class certification, or at any other time, based on, inter alia, changing circumstances and/or new facts obtained.

65. **Numerosity**. On information and belief, hundreds of thousands of consumers fall into the definitions of the Class. Members of the Class can be identified through Defendant's records, discovery, and other third-party sources.

66. **Commonality and Predominance**. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual members of the Class. These common legal and factual questions include, but are not limited to, the following:

a. Whether Defendant's sale of geolocation data without consent constitutes unjust enrichment;

b. Whether Defendant's conduct violates state consumer protection statutes;

c. Whether Plaintiff and the other Class members were damaged by Defendant's conduct; and

d. Whether Plaintiff and the other Class members are entitled to restitution or other relief.

67. **Typicality**. Plaintiff's claims are typical of the claims of the other members of the Class in that, among other things, all Class members were similarly situated and were comparably injured through Defendant's wrongful conduct as set forth herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

68. **Adequacy of Representation**. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel that is highly experienced in complex consumer class action litigation, and Plaintiff intends to vigorously prosecute this action on behalf of the Class. Furthermore, Plaintiff has no interests that are antagonistic to those of the Class.

69. **Superiority**. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense of individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class to obtain effective redress for the wrongs committed against the members on an individual basis. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances.

70. Further, Defendant has acted and refused to act on grounds generally applicable to the proposed Class, thereby making appropriate final injunctive and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

COUNT I
Unjust Enrichment
(On behalf of Plaintiff and the Class)

71. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

72. Plaintiff brings this claim individually and on behalf of members of the Class and the Florida Subclass against Defendant.

73. To the extent required by law, Plaintiff brings this claim in the alternative to any legal claims that may be alleged.

74. Plaintiff also alternatively alleges this claim as a Quasi-Contract or Non-Quasi-Contract Claim for Restitution and Disgorgement.

75. Plaintiff and Class members unwittingly conferred a benefit upon Defendant. Defendant acquired valuable personal location information belonging to Plaintiff and Class members which it then sold to other parties without the consent of Plaintiff and Class members. Plaintiff and Class members received nothing from this transaction. Plaintiff lacks an adequate remedy at law, and pleads this cause of action in the alternative to the extent Plaintiff is required to do so.

76. Defendant has knowledge of such benefits.

77. Defendant has been unjustly enriched in retaining the revenues derived from the sale of Plaintiff's and Class members' data, including their geolocation data. Retention of those moneys under these circumstances is unjust and inequitable because Defendant did not obtain the meaningful consent of Plaintiff and Class members before selling their data to third parties as described above.

78. Because Defendant's retention of the non-gratuitous benefits conferred on it by Plaintiff and Class members is unjust and inequitable, Defendant must pay restitution to Plaintiff and the Class members for its unjust enrichment, as ordered by the Court.

79. Plaintiff and the members of the Class lack an adequate remedy at law to address the unfair conduct at issue here. Legal remedies available to Plaintiff and class members are inadequate because they are not equally prompt and certain and in other ways efficient as equitable relief. Damages are not equally certain as restitution because the standard that governs restitution is different than the standard that governs damages. Hence, the Court may award restitution even if it determines that Plaintiff fails to sufficiently adduce evidence to support an award of damages. Damages and restitution are not the same amount. Unlike damages, restitution is not limited to the amount of money a defendant wrongfully acquired plus the legal rate of interest. Equitable relief, including restitution, entitles the plaintiff to recover all profits from the wrongdoing, even where

the original funds taken have grown far greater than the legal rate of interest would recognize. Legal claims for damages are not equally certain as restitution because claims for restitution entail few elements. In short, significant differences in proof and certainty establish that any potential legal claim cannot serve as an adequate remedy at law.

80. Plaintiff and members of the putative class seek non-restitutionary disgorgement of the financial profits that Defendant obtained as a result of its unjust conduct.

PRAYER FOR RELIEF

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

a. For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as the representative for the Class and Plaintiff's attorneys as Class Counsel;

b. For an order declaring that Defendant's conduct violates the laws referenced herein;

c. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

d. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

e. For prejudgment interest on all amounts awarded;

f. For an order of restitution and all other forms of equitable monetary relief;

g. For injunctive relief as the Court may deem proper; and

h. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

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

Dated: January 12, 2023

BURSOR & FISHER, P.A.

By: /s/ *Joel D. Smith*
Joel D. Smith

Joel D. Smith (SBN 244902)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: jsmith@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

Attorneys for Plaintiff