

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Lina M. Khan, Chair
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson**

In the Matter of

GRAVY ANALYTICS, INC., a corporation,

and

VENNTEL, INC., a corporation.

DOCKET NO.

COMPLAINT

The Federal Trade Commission, having reason to believe that Gravy Analytics, Inc., a corporation, and Venntel, Inc., a corporation, (collectively, “Respondents”), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Gravy Analytics, Inc. (“Gravy Analytics”) is a Delaware corporation with its principal office or place of business at 44679 Endicott Dr Suite 300, Ashburn, VA 20147.
2. Respondent Venntel, Inc. (“Venntel”) is a Delaware corporation with its principal office or place of business at 2201 Cooperative Way, Suite 600, Herndon, Virginia 20171. Venntel is a wholly-owned subsidiary of Gravy Analytics.
3. Respondents have bought, obtained, and collected precise consumer location data and offered for sale, sold, and distributed products and services created from or based on the consumer location data.
4. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

Respondents' Business Practices

5. Mobile phones are ubiquitous in the daily lives of Americans. Most consumers report keeping their phones near them at all times, meaning that their phones go everywhere that they go. These devices are able to constantly track a user's location, generating records of a user's whereabouts throughout the day. Mobile phones are a source of personal information about their users, including personal information in the form of this location data.
6. Location data can expose sensitive information such as medical conditions, sexual orientation, political activities, and religious beliefs. When collected across time, this data can reveal every aspect of a consumer's life. Indeed, Respondents make this point in marketing material to potential customers, asserting that "Where we go is who we are." This is more than just an advertising slogan for Respondents – it is the very point of their business.
7. Respondents amass and sell raw location data that tracks consumers' movements so that their customers can glean insights into consumers' private lives. In addition, Gravy Analytics also uses this data to identify consumers based on attributes and behaviors the data reveals, including sensitive and personal attributes and behaviors, and it then discloses this information to third parties.
8. Respondents do not collect mobile location data directly from consumers. Indeed, consumers generally have no interactions with Respondents and have no idea that Respondents have obtained their location data.
9. Respondents obtain consumer location data from other data suppliers. These suppliers may themselves obtain the location data from other data suppliers, the mobile advertising marketplace, or mobile applications. Through these various suppliers, Respondents claim to "collect, process and curate" over 17 *billion* signals from approximately a *billion* mobile devices on a *daily* basis.
10. These location signals, gathered from consumers' mobile phones, identify consumers' precise geolocation by latitude and longitude coordinates at the time the signal was gathered. Each location signal is also associated with a Mobile Advertising ID ("MAID") which is an alphanumeric identifier that iOS or Android platforms assign to each mobile device. This unique mobile device identifier is assigned to a consumer's mobile phone to assist marketers in advertising to consumers. These data signals are collected from a mobile device's GPS coordinates and may, at times, be augmented by other signals, such as WiFi.
11. The precision of the location signals gathered by Respondents is high. In its support documentation, Gravy Analytics states that location signals "should be at least 5 decimal places of precision." The more decimal points in a location signal, the more precise the signal is. At 5 decimal points, the signal identifies a consumer's location to within approximately one meter of precision. This means the signal is sufficiently precise to identify not only what building a consumer is visiting, but even what room the consumer is in.
12. Respondents also tout the accuracy of their data. For example, Respondents assert that they have "implemented algorithms that process billions of data points daily [and] filter out

unreliable signals,” thus leaving Respondents with only data signals that they have been “verified as accurate.” Respondents also explain that, when associating a data signal with a location, they use hand-drawn polygons (that is, using employees to draw the shape of the location being tracked) that “traces the walls of the venue,” so that their data is “based on real people visiting real locations” without any “modeling.”

Respondents Disclose Consumers’ Precise Geolocation Information that Tracks Consumers to Sensitive Locations

13. Respondents’ business model is to compile massive amounts of mobile geolocation data collected from consumers and then disclose this information to third parties for a price. Gravy Analytics focuses on selling this information to commercial customers, while its subsidiary, Venntel, sells the information to public sector customers.

14. Respondents deliver data to their customers through file transfers at regular intervals, such as daily or weekly, or through providing access through an Application Programming Interface (“API”). In addition to continuously updating with new data, Respondents offer their customers the opportunity to search and receive at least three years of historical data.

15. Gravy Analytics sells multiple data products based on the consumer geolocation data it has compiled. For example, Gravy Analytics transfers raw precise mobile location data – that is timestamped latitude and longitude coordinates tied to, among other things, a MAID (or another persistent identifier) and IP address – to customers via batch deliveries through the cloud. Gravy Analytics offers data from as recent as the prior 48 hours to the previous year. Customers are able to schedule batch deliveries of location data based on requested criteria, such as geographic area or time.

16. Gravy Analytics also sells a tool that allows a marketer to “geo-fence” a location and obtain a list of MAIDs that were present at that location during a specific timeframe. For example, using this tool, a Gravy Analytics’ customer could generate a list of MAIDs that attended a private event for a political cause. Gravy Analytics itself has used geo-fencing to create a list of MAIDs that visited specific churches and health-related events for customers.

17. Another tool tracks MAIDs that attend certain events, such as concerts or sporting events. Gravy Analytics asserts it “monitor[s] 1M+ local events.”

18. Gravy Analytics also transfers location data to its subsidiary, Venntel. Venntel sells the information to public sector customers, such as government contractors. Venntel sells location data associated with, among other things, a MAID or other persistent identifier, timestamp, IP address, and name of the app from which the location was collected.

19. Venntel also provides enhanced tools to its public sector customers to analyze and access consumers’ location data. When a customer accesses Venntel’s data using one of these enhanced tools, Venntel typically associates the data with a unique persistent identifier that it refers to as a Venntel ID (“VID”). Venntel offers a tool that converts VIDs into MAIDs (and vice versa). Thus, the VID does not provide protections for consumers.

20. Examples of the enhanced tools provided by Venntel include:

- Allow customers to geo-fence specific locations and collect VIDs that enter the location, along with IP addresses and timestamps, among other information, associated with the identifier;
- “Continuously” track a single device;
- Obtain device information about the mobile device associated with a VID, such as operating system, device brand, carrier type, and IP address; and
- Search location signals associated with specific IP addresses.

21. Venntel markets to its public sector customers that the location data and these enhanced tools can be used for government purposes.

22. The precise geolocation data, associated with MAIDs or other persistent identifiers, licensed, used, and sold by Respondents could 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, political activity, and welfare and homeless shelters. Indeed, as alleged below, Respondents themselves have tracked consumers to sensitive locations, including places of worship, political rallies, and locations associated with medical conditions or decisions.

The Data Sold by Respondents Is Individually Identifiable

23. The location data collected, used, and sold by Respondents identifies individual consumers and is not anonymized. A persistent identifier, such as a MAID, is personally identifiable information. Respondents’ geolocation data, combined with the mobile device’s MAID or other persistent identifiers, identifies the mobile device’s user or owner. Such identification occurs through several different methods.

24. *First*, the location data that Respondents collect, use, and sell typically includes multiple timestamped signals for each MAID or other persistent identifiers, which identifies many details about the mobile device owners.

25. For example, Venntel tells potential customers that “location data makes it possible to gain real-life insight into a device users’ patterns-of-life (POL), locations visited and known associates.” Venntel further explains that, over a 90-day tracking of a “VIP Device,” the company was able to identify the device user’s “bed down location, work location, and visits to other USG [United States Government] buildings.” Additionally, in a “Quick Guide” document for one of its services, Venntel notes that where a device is located during the evening hours will show its customers when the consumer is at “home, gym, evening school, etc.”

26. Indeed, companies and other entities are using precise geolocation data to identify consumers and their activities. In one well-publicized example, a group used precise mobile geolocation data to identify by name a Catholic priest who visited LGBTQ+-associated locations, thereby exposing the priest’s sexual orientation and forcing him to resign his position. As another example, journalists who purchased precise mobile geolocation from a data broker were able to track consumers over time and, as a result, identify several consumers, including

military officials, law enforcement officers, and others. One person the journalists were able to identify by name (and who confirmed her identity) was tracked attending a prayer service at a church.

27. *Second*, MAIDs and other persistent identifiers, by design, enable direct communication with individual consumers, are used to amass profiles of individuals over time and across different web and mobile services, and are the basis to make decisions and insights about individual consumers.

28. *Third*, Gravy Analytics also encourages its customers to add Gravy Analytics' data to what the customers already know about consumers. For example, Gravy Analytics explains that its customers can “[a]ppend [Gravy Analytics'] customer behavioral information to your C[ustomer] R[elationship] M[anagement] data.” CRM is a tool in which companies maintain information about and interactions with customers. Gravy Analytics even brags that when a company matches its own customer data to Gravy Analytics' database, that “60% of customers [are] recognized” in Gravy Analytics' database.

29. To make it even more explicit, Gravy Analytics suggested to one retail customer that appending Gravy Analytics' data to the customer's CRM data could “[c]onnect online to offline” – that is, “[u]nderstand which of your online shoppers visit your stores and vice-versa – whether or not they buy – for a fuller customer profile.”

30. *Finally*, many businesses link consumers' MAIDs to other information about them, such as names, addresses, email addresses, and phone numbers. Indeed, at least one data broker that supplies geolocation data to Gravy Analytics specifically advertises a service that connects MAIDs to these other personally identifying points of information. Other data brokers advertise similar products.

Consumers Have Not Consented to Gravy Analytics' and Venntel's Collection, Use, or Sale of Their Mobile Location Data and Respondents Fail to Take Reasonable Steps to Confirm Consent

31. The precise mobile location data collected, used, and sold by Respondents is sensitive information. As Respondents know and understand, consumers must provide consent to the collection and use of consumers' location data. Gravy Analytics has recognized this in business documents, including in a survey it provides to its suppliers, which states:

7. If you provide to Gravy Personal Data collected in the United States, do you (or your data suppliers):
 - a. Obtain affirmative, express Consent to collect “sensitive information”¹ in accordance with FTC guidance: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>?
 - b. Obtain verifiable parental Consent, as required under COPPA, if you provide Gravy with Personal Data from US data subjects ages 13 and under?
8. If you collect and/or receive Personal Data collected in the EU/EEA and are established in the U.S. or other country determined by the EU not to have adequate data protection, what transfer mechanism do you use? Please describe.

Data Subject Rights

¹ Please note that precise geolocation data is considered by the FTC to be “sensitive data”.

32. Despite understanding that precise geolocation data is sensitive information that requires consumers’ consent, Respondents fail to take reasonable steps to confirm consumers consented to Respondents’ collection, use, or sale of this data and consumers do not, in fact, consent to the collection, use, and sale of their location data by Respondents.

33. Although Gravy Analytics requests its suppliers to provide samples of notices that are presented to consumers, Gravy Analytics continues to collect, use, and sell data provided by the supplier even if a supplier refuses to provide this information.

34. In other instances, Gravy Analytics continued to use data obtained from data suppliers that provided ambiguous or non-responsive information to Gravy Analytics’ questionnaires. For example, in its questionnaire, Gravy Analytics asked a data supplier what the data supplier required consumers to agree to in their consent framework. The data supplier failed to provide any response about the information it collected from American consumers and only explained what the supplier required of European consumers:

To what specifically does the data subject Consent? (i.e. collection and transfer for specific purposes or just collection of the data?) → Depending on the countries → for EU they consent to all different IAB purposes + all partners getting Access to the data

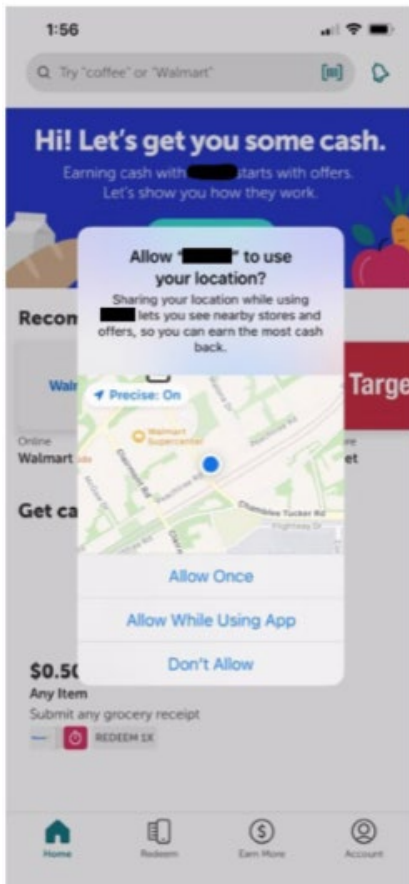
35. As another example, in response to a questionnaire asking whether the data supplier obtains consent from consumers, the data supplier responded that its mobile applications collect consent “[w]herever applicable regulatory rules dictate” without any explanation as to when or where the supplier believed such “regulatory rules dictate” or the parameters of the regulatory rules.

36. Despite these ambiguous or non-responsive answers, Gravy Analytics continued to use data obtained from these sources.

37. Venntel does not have any processes in place to confirm that consumers are appropriately consenting to the collection, use, or sale of their location data for government purposes. Instead, Venntel relies on Gravy Analytics to obtain such confirmations, which, as alleged above, it fails to do.

38. Moreover, in some instances, Respondents continue to use consumers’ location data even after learning that consumers have not provided informed consent.

39. Respondents have regularly purchased location information to use for purposes wholly unrelated to the purpose that consumers were told that their location information would be used. For example, in onboarding a new data supplier, the new data supplier provided Gravy Analytics with the following example of how consumer consent was obtained:

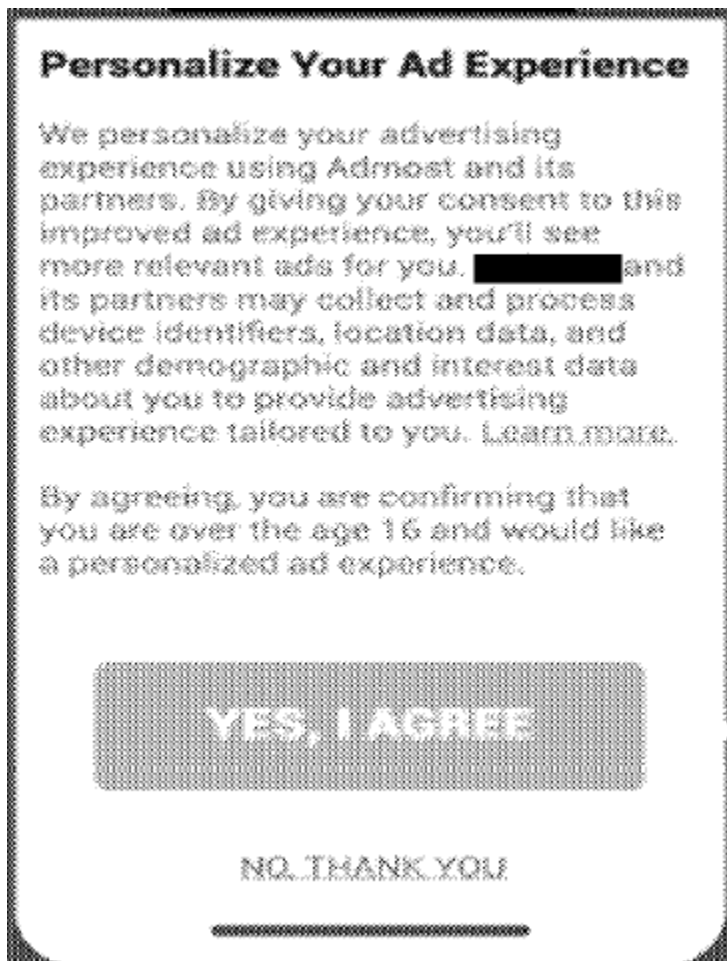


In this consent screen, the consumer is lured in with the message “Let’s get you some cash” and is told they should share their location to “see nearby stores and offers, so you can earn the most cash back.”

40. In this example, the consent screen does not explain to consumers that their location data will be sold to third-party data brokers. It also does not disclose any of the uses to which Gravy Analytics, or its customers, will put the data, including categorizing consumers based on their behaviors, targeted advertising, and selling it to the government.

41. As another example, one data supplier described to Gravy Analytics the data it would provide as “collected from mobile applications where the user of the mobile application has opted in for third[-]party marketing, ad targeting, predictive modeling and analytics.” Although this description revealed that the data supplier was not obtaining consent from consumers to use their location data for government purposes, Gravy Analytics still shared this information with Venntel to sell to public sector customers for those purposes.

42. The same supplier provided Gravy Analytics with examples of notices used to collect consent from consumers. These examples confirmed that the supplier was not obtaining consent from consumers for their location data to be used for government purposes. For example, one such notice stated:



43. As another example, in response to a question about the consent that a data supplier obtains from consumers, the data supplier responded merely that consent is obtained for, “collection and the transferring to named 3rd-parties.” This consent framework fails to explain to consumers that their information may be used for commercial purposes or government purposes. Moreover, Gravy Analytics was aware that it was not one of the named third parties. Yet, Gravy Analytics continued to use, and provide to Venntel, data obtained from this data supplier.

Gravy Analytics Targets Consumers Based on Sensitive Characteristics and Behaviors

44. Gravy Analytics explains to its customers that the mobile geolocation data it collects and sells not only reveals where consumers go and what they do, but also may be used for “psychographic analysis” – that is, analysis to understand consumers’ “values, interests, [and] lifestyles.” Indeed, Gravy Analytics insists that its location data is “deterministic.”

45. In addition to peddling its data for this use, Gravy Analytics itself engages in such analysis to create additional data products to sell to its customers. Gravy Analytics analyzes the location data it obtains in order to create additional data points to sell to its customers. For example, Gravy Analytics uses the data it collects to create “audience segments,” or subsets of consumers who share interests or characteristics, including audience segments based on sensitive interests or characteristics. These groupings are formed based on the locations and events visited by mobile devices, combined with other information gathered about consumers, and allow Gravy Analytics’ customers to identify and target consumers based on identified sensitive and personal interests or characteristics.

46. Gravy Analytics offers over 1100 audience segments with each segment made up of a list of MAIDs of consumers that meet the targeted interest or characteristic.

47. Gravy Analytics builds audience segments about practically every aspect of a consumer’s life, including their employment, personal habits, and retail activity. For example, Gravy Analytics has offered audience segments such as “Early Risers,” “Sports Betting Enthusiast,” “McDonald’s Breakfast Diners,” “Healthy Dads,” “Restaurant Visitor during COVID Quarantine,” and “Lingerie Retail Shoppers.”

48. Other segments are based on health or medical decisions made by consumers. For example, Gravy Analytics has offered audience segments such as “New Parents/Expecting,” “Women’s Health,” “CBD [cannabidiol] Shoppers,” “Elder Care Interest,” and “Pharmacy Visitor during COVID Quarantine.” As one example of how Gravy Analytics builds such audience segments, Gravy Analytics explains that its “New Parents/Expecting” segment includes consumers who are “attending Lamaze, birthing, breastfeeding, new parent support groups, etc. events.”

49. Other segments are built on information about a consumer’s family. For example, Gravy Analytics has offered audience segments such as “Stay at Home Parents,” “Parents with Young Kids,” “Parents of High School Students,” and “In-Market Insurance Buyers,” which includes consumers identified as, among other things, “getting married” and “having children” “based on events and places they visit.” Likewise, Gravy Analytics explains that, as part of its persona data

product, consumers “observed at toy stores and children’s events” could have the “Stay-at-Home Parents” segment attached to their MAID.

50. Yet other segments are based on political activity. For example, Gravy Analytics has offered audience segments such as “Political Activist,” “Likely Republican Voter,” and “Likely Democrat Voter.” Gravy Analytics explains that the “Likely Republican Voter” segment is based on consumers “attending Republican focused political events and events and venues affiliated with conservative topics.”

51. In addition to providing a catalogue of standard audience segments, the company also advertises custom audience segments and has created them for customers with special requests, including custom audience segments based on sensitive characteristics of consumers.

52. For example, Gravy Analytics geo-fenced breast cancer-related events and identified the MAIDs of consumers attending those events for a customer.

53. In another example, Gravy Analytics geo-fenced specific churches and provided its customer with MAIDs of churchgoers at those churches, the dates of each visit, and which church each consumer visited. Gravy Analytics also categorized the MAIDs by frequency of attendance. The custom audience segments included:

Name of Custom Audience	Description of Audience*
1. Minnesota Christian Churchgoers Light	<ul style="list-style-type: none"> Attendees of Christian churches based in Minnesota who frequent only a few times over the period of measurement
2. Minnesota Christian Churchgoers Heavy	<ul style="list-style-type: none"> Attendees of Christian churches based in Minnesota who frequent many times over the period of measurement
3. Wisconsin Christian Churchgoers Light	<ul style="list-style-type: none"> Attendees of Christian churches based in Wisconsin who frequent only a few times over the period of measurement
4. Wisconsin Christian Churchgoers Heavy	<ul style="list-style-type: none"> Attendees of Christian churches based in Wisconsin who frequent many times over the period of measurement
5. Charlotte Christian Churchgoers Light	<ul style="list-style-type: none"> Attendees of Christian churches based in Charlotte, NC who frequent only a few times over the period of measurement
6. Charlotte Christian Churchgoers Heavy	<ul style="list-style-type: none"> Attendees of Christian churches based in Charlotte, NC who frequent many times over the period of measurement
7. Atlanta Christian Churchgoers Light	<ul style="list-style-type: none"> Attendees of Christian churches based in Atlanta, GA who frequent only a few times over the period of measurement
8. Atlanta Christian Churchgoers Heavy	<ul style="list-style-type: none"> Attendees of Christian churches based in Atlanta, GA who frequent many times over the period of measurement

54. As another example, Gravy Analytics tracked consumers at United States Postal Services, Veteran Health Administration, and Veterans Affairs offices in four states for a customer.

55. In addition, if a customer wishes to get specific information about individual consumers, Gravy Analytics also offers a “persona” data product in which it will provide a list of every audience segment connected to a specific MAID. For example, using the “persona” data product, a Gravy Analytics’ customer could learn that a specific device MAID (e.g., 1234ABCD-1234-ABCD-1234-ABCD1234ABCD) is classified in the Gen X, Blue Collar Worker, ATM visitor, Parent of Teenagers, Golf Enthusiast, and Medicare Interest audience segments. Gravy Analytics claims to have associated over 250 million MAIDs of consumers with at least one audience segment.

Respondents Cause Substantial Injury to Consumers by Invading Consumers' Privacy

56. Respondents collect, use, and sell precise location data that invades consumers' privacy. This data provides a comprehensive picture of consumers' private lives – for example, where they live, eat, and work. It could be used to identify medical facilities and places of worship visited by the consumer, other individuals with whom the consumer is associating, and habitual movements such as commuting routes and daily patterns. The precision and comprehensive nature of this data is such that it reveals information about and details of consumers' lives that cannot be obtained through physical observations of public spaces.

57. Gravy Analytics has also used the precise geolocation to track consumers to sensitive locations, such as events associated with medical conditions, religious worship, and political activity. Gravy Analytics further uses this information to categorize consumers based on sensitive attributes, such as medical decisions or political activity.

58. Respondents' invasion of privacy affects millions of consumers. Respondents claim to process location data from over a billion mobile devices on a daily basis. Respondents likewise claim to associate at least 250 million MAIDs with at least one interest or attribute. In addition, Gravy Analytics tracked 306,648 MAIDs *in a single day* in connection with the audience segment in which it tracked consumers at United States Postal Service, Veterans Health Administration, and Veteran Affairs offices, as alleged above in Paragraph 54. Other audience segments prepared by Gravy Analytics, in which the company tracked consumers for longer periods of time, include millions of MAIDs.

59. Because of the sensitive information such data reveals, Respondents' unauthorized collection, use, and sale of precise geolocation data is an unwarranted intrusion into consumers' privacy and causes substantial injury to consumers.

Respondents Cause or Are Likely to Cause Consumers to Suffer from Stigma, Discrimination, Physical Violence, Emotional Distress, and Other Harms

60. In addition to invading consumers' privacy, Respondents' practices cause or are likely to cause other forms of injury to consumers, including stigma, discrimination, physical violence, emotional distress, and other harms.

61. For example, through Respondents' precise geolocation data, Respondents' customers are able to target consumers who have visited sensitive locations, exposing the consumers to these additional injuries.

62. Respondents' precise geolocation data is not anonymous. Respondents associate their precise geolocation data with unique persistent identifiers, including MAIDs. MAIDs and similar persistent identifiers are personally identifiable information as, among other things, they allow companies to track and contact individual consumers. MAIDs and similar persistent identifiers also allow companies to build profiles of consumers' activities over time.

63. In addition, identifying consumers by name or other identifying information from Respondents' geolocation data is straightforward, whether through tracking their movements or by using services that connect MAIDs to names and other personally identifying information.

64. In fact, identifying and targeting consumers based on precise geolocation collected from mobile devices does occur. For example, a Catholic priest was outed and forced to resign his position based on location data that was collected from his mobile device and then sold to a group who used it to track priests' movements.

65. Gravy Analytics' audience segments, including the ones that identify consumers based on sensitive characteristics, are also associated with MAIDs. As alleged above, MAIDs can be connected by data brokers to other personally identifying information, such as names, addresses, and email addresses. Gravy Analytics thus sells or has sold data that associates consumers to sensitive characteristics, such as medical decisions, political activity, and religious practices. Unauthorized disclosure of such sensitive characteristics puts individuals at significant risk of stigma, discrimination, physical violence, emotional distress, and other harms.

66. Even without connecting a MAID to a consumer's name or other personally identifying information, the MAID itself is used to target consumers based on a particular interest or characteristic. MAIDs are unique personal identifiers that advertisers and advertising platforms use to identify a device to send a targeted advertisement. Indeed, targeting individual consumers is the MAIDs' primary purpose and MAIDs may be used to harm consumers.

67. Such targeting and harm occur in the data marketplace. For example, the Massachusetts Attorney General brought a law enforcement action in 2018 against a data broker that sent targeted advertisements about abortion and alternatives to abortion to the broker's "abortion-minded women" audience segment using consumers' MAIDs. The "abortion-minded women" audience segment was identified as consumers who, according to their precise geolocation, were "close to or entered the waiting rooms of women's reproductive health clinics." The data broker collected these consumers' MAIDs and used them to serve the consumers the targeted ads.

68. As another example, another group advertised the ability to reach "abortion-vulnerable women" by capturing the "the cell phone IDs [i.e. MAIDs] of women coming and going from Planned Parenthood and similar locations and then serv[ing] them life-affirming ads" online using those MAIDs. According to news reports, one such ad read, "Took the first pill at the clinic? It may not be too late to save your pregnancy." According to the reports, the ads pointed consumers to websites that attempted to persuade consumers to attempt a scientifically unsupported "abortion reversal" procedure. The group further alarmingly asserted on its website that its product "takes the guesswork out of the marketing equation" because its customers will "no longer have to wonder if women can find *you*. Now, you'll find *them*!" The ads served by the group were seen 14.3 million times.

69. The data and data products sold by Respondents, including consumers' precise geolocation data and audience segments, identify sensitive characteristics about consumers and cause or are likely to cause substantial injury in the form of stigma, discrimination, physical violence, emotional distress, and other harms.

The Substantial Injury Caused by Respondents' Actions Is Not Reasonably Avoidable by Consumers or Outweighed by Countervailing Benefits

70. The collection and use of data collected from the mobile devices are opaque to consumers, who typically do not know who has collected their data or how it is being used. To the extent that consumers opt-in to the collection of precise geolocation from their devices, such opt-in processes typically do not explain to the consumer that Respondents will receive the data, how they will use the data, or that it will be further disclosed to additional third parties unknown to the consumer. Indeed, as alleged above, in many instances, consumers believe or are told they are opting into data collection for wholly different purposes.

71. Once information is collected about consumers from their mobile devices or other sources, the information can be and, in many instances, is provided multiple times to companies that consumers have never heard of and never interacted with. Consumers have no insight into how their data is used. Consumers are therefore unable to take reasonable steps to avoid the above-described injuries.

72. Respondents could implement safeguards to protect consumer privacy, such as blacklisting sensitive locations from all of their data products or removing all audience segments based on sensitive characteristics from their data products. Such safeguards could be implemented at a reasonable cost and expenditure of resources. Thus, the harms described above are not outweighed by countervailing benefits to consumers or competition.

Count I
(Both Respondents)
Unfair Sale of Sensitive Data

73. In numerous instances, Respondents have sold, licensed, or otherwise transferred precise geolocation data associated with unique persistent identifiers that reveal consumers' visits to sensitive locations.

74. Respondents' acts or practices 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.

75. Therefore, Respondents' acts or practices as set forth in Paragraph 74 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

**Count II
(Both Respondents)**

Unfair Collection and Use of Consumer Location Data Without Consent Verification

76. In numerous instances, Respondents have collected consumers' location data without taking reasonable steps to verify that consumers provide informed consent to Respondents' collection, use, or sale of the data for commercial and government purposes.

77. Respondents' acts or practices 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.

78. Therefore, Respondents' acts or practices as set forth in Paragraph 77 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

**Count III
(Gravy Analytics)**

Unfair Sale of Sensitive Inferences Derived from Consumers' Location Data

79. In numerous instances, Gravy Analytics has categorized consumers into audience segments based on sensitive characteristics, such as medical conditions, political activities, and religious beliefs, derived from location data. It has sold these audience segments to third parties.

80. Gravy Analytics' acts or practices 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.

81. Therefore, Gravy Analytics' acts or practices as set forth in Paragraph 80 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

Violations of Section 5

82. The acts and practices of Respondents as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this _____ day of _____, 2024, has issued this Complaint against Respondents.

By the Commission.

April J. Tabor
Secretary

SEAL: