212-3035

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. C-4810**

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

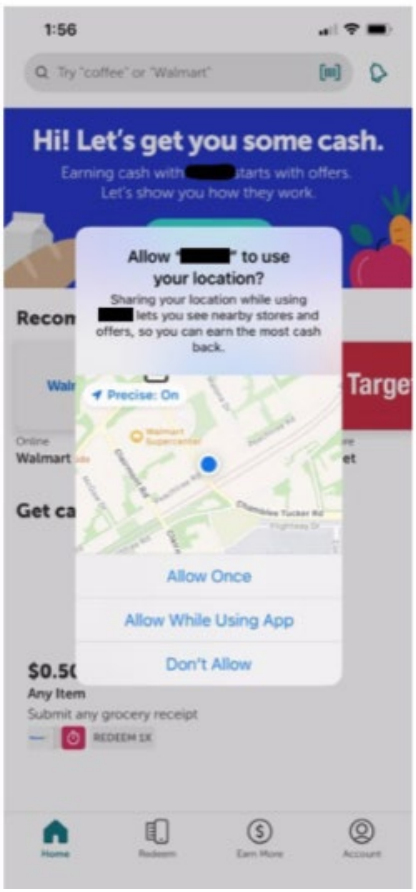
35. As another example, in response to a questionnaire asking whether the data supplier obtains consent from consumers, the data supplier responded that its mobile applications collect consent "[w]herever applicable regulatory rules dictate" without any explanation as to when or where the supplier believed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

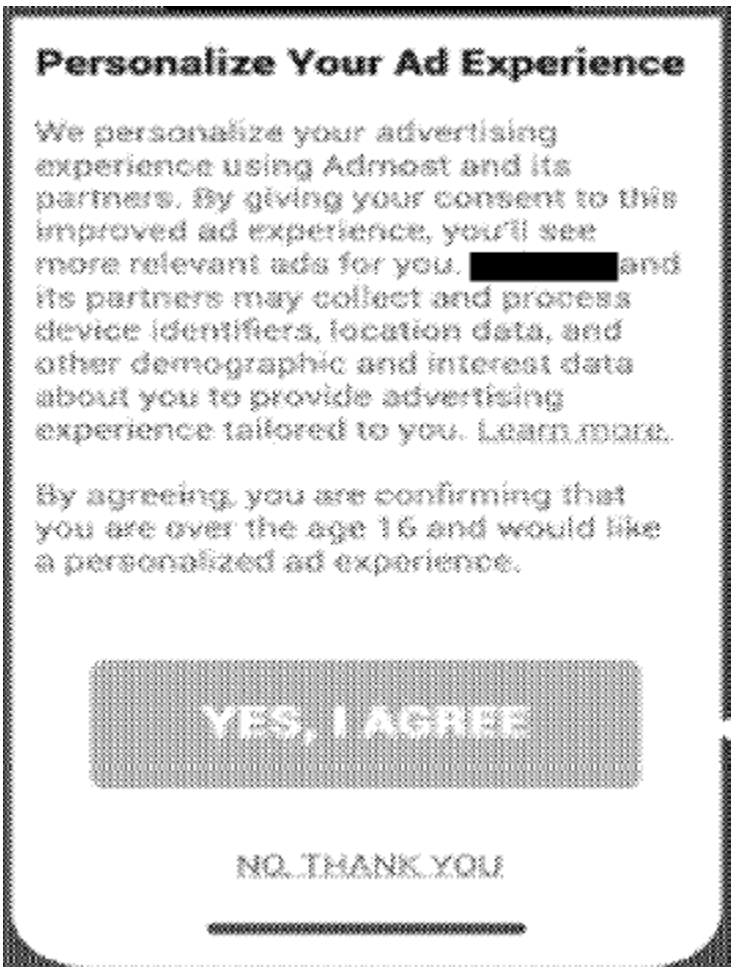


In this consent screen, the consumer is lured in with the message "Let's get you some cash" and is told they should share their location to "see nearby stores and offers, so you can earn the most cash back."

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 suppler.

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	• Attendees of Christian churches based in Minnesota who frequent only a few times over the period of measurement
2. Minnesota Christian Churchgoers Heavy	• Attendees of Christian churches based in Minnesota who frequent many times over the period of measurement
3. Wisconsin Christian Churchgoers Light	• Attendees of Christian churches based in Wisconsin who frequent only a few times over the period of measurement
4. Wisconsin Christian Churchgoers Heavy	• Attendees of Christian churches based in Wisconsin who frequent many times over the period of measurement
5. Charlotte Christian Churchgoers Light	• Attendees of Christian churches based in Charlotte, NC who frequent only a few times over the period of measurement
6. Charlotte Christian Churchgoers Heavy	• Attendees of Christian churches based in Charlotte, NC who frequent many times over the period of measurement
7. Atlanta Christian Churchgoers Light	• Attendees of Christian churches based in Atlanta, GA who frequent only a few times over the period of measurement
8. Atlanta Christian Churchgoers Heavy	• 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 13th day of January, 2025, has issued this Complaint against Respondents.

By the Commission.

April J. Tabor
Secretary

SEAL:

UNITED STATES OF AMERICA **212-3035**
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.**	**DECISION AND ORDER** **Docket No. C-4810**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe Respondents had violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

The Respondents are:

a. Respondent Gravy Analytics, Inc., a Delaware corporation with its principal office or place of business at 44679 Endicott Dr Suite 300, Ashburn, VA 20147.

b. Respondent Venntel, Inc., 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.

The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For the purpose of this Order, the following definitions apply:

A. "**Affirmative Express Consent**" means any freely given, specific, informed, and unambiguous indication of an individual consumer's wishes demonstrating agreement by the individual, such as by an affirmative action, following a Clear and Conspicuous Disclosure to the individual of: (1) the categories of information that will be collected; (2) the purpose(s) for which the information is being collected, used, or disclosed; (3) the hyperlink to a document that describes the types of entities to whom the Covered Information is disclosed; and (4) the hyperlink to a simple, easily-located means by which the consumer can withdraw consent and that Clearly and Conspicuously describes any limitations on the consumer's ability to withdraw consent. The Clear and Conspicuous Disclosure must be separate from any "privacy policy," "terms of service," "terms of use," or other similar document.

The following does not constitute Affirmative Express Consent:

1. Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the consumer; or

2. Obtaining consent through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice.

B. "**Clear(ly) and Conspicuous(ly)**" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made through only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

C. "**Covered Information**" means information from or about an individual consumer including, but not limited to: (1) a first and last name; (2) Location Data; (3) an email address or other online contact information; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other government-issued identification number; (7) a financial institution account number; (8) credit or debit card information; (9) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; or (10) socio-economic or demographic data. Deidentified information is not Covered Information.

D. "**Data Product**" means any model, algorithm, or derived data, in Respondents' custody or control, developed, in whole or part, using Historic Location Data. Data Product includes but is not limited to any derived data produced via inference (manual or automated) or predictions such as audience segments.

E. **"Deidentified" or "Deidentifiable"** means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person, in that Respondents must, at a minimum:

1. Have implemented technical safeguards that prohibit reidentification of the person to whom the information may pertain;

2. Have implemented business processes that specifically prohibit reidentification of the information, including by buyers, customers, or other entities to whom Respondents provide the information;

3. Have implemented business processes to prevent inadvertent release of Deidentified information; and

4. Make no attempt to reidentify the information.

F. **"Historic Location Data**" means any Location Data that Respondents collected from consumers without consumers' Affirmative Express Consent.

G. "**Location Data**" means any data that may reveal a mobile device's or consumer's precise location, including but not limited to Global Positioning System (GPS) coordinates, cell tower information, or precise location information inferred from basic service set identifiers (BSSIDs), WiFi Service Set Identifiers (SSID) information, or Bluetooth receiver information, and any unique persistent identifier combined with any such data, such as a mobile advertising identifier (MAID) or identifier for advertisers (IDFA). Data that: (1) reveals only a mobile device or consumer's coarse location data (e.g., zip code or census block location with a radius of at least 1,850 feet), or (2) is used for (a) Security Purposes, (b) National Security purposes conducted by federal agencies or other federal entities, or (c) response by a federal law enforcement agency to an imminent risk of death or serious bodily harm to a person, is not Location Data.

H. "**National Security"** means the national defense, foreign intelligence and counterintelligence, international and internal security, and foreign relations. This includes countering terrorism; combating espionage and economic espionage conducted for the benefit of any foreign government, foreign instrumentality, or foreign agent; enforcing export controls and sanctions; and disrupting cyber threats that are perpetrated by nation states, terrorists, or their agents or proxies.

I. "**Raw Format**" means the format in which Location Data is originally supplied, prior to any form of processing, extraction, or analysis taking place.

J. "**Respondents**" means Gravy Analytics, Inc. ("Gravy") and Venntel, Inc. ("Venntel"), and their successors and assigns.

K. "**Security Purposes"** means preventing, detecting, protecting against, or responding to data security incidents, including cybersecurity incidents, identity theft, fraud, phishing, harassment, malicious or deceptive activities, or preserving the integrity or security of systems.

L. "**Sensitive Locations**" means locations within the United States associated with: (1) medical facilities (e.g., family planning centers, general medical and surgical hospitals, offices of physicians, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, outpatient care centers, psychiatric and substance abuse hospitals, and specialty hospitals); (2) religious organizations; (3) correctional facilities; (4) labor union offices;

(5) locations of entities held out to the public as predominantly providing education or childcare services to minors; (6) associations held out to the public as predominantly providing services based on racial or ethnic origin; (7) locations held out to the public as providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; or (8) military installations, offices, or buildings.

M. "**Sensitive Location Data**" means any consumer Location Data associated with a Sensitive Location.

N. "**Third-Party Incident**" means the sharing by a third party of Respondents' Location Data, in violation of a contractual requirement between Respondents and the third party.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Respondents and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, promotion, offering for sale, sale, or distribution of any product or service, must not misrepresent, in any manner, expressly or by implication:

A. The extent to which Respondents review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt in controls;

B. The extent to which Respondents collect, use, maintain, disclose, or delete any Covered Information; and

C. The extent to which the Location Data that Respondents collect, use, maintain, or disclose is Deidentified.

II. Prohibitions on the Use, Sale, or Disclosure of Sensitive Location Data

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, and employees, whether acting directly or indirectly, must not sell, license, transfer, share, disclose, or otherwise use in any products or services Sensitive Location Data associated with the Sensitive Locations that Respondents have identified within 90 days of the effective date of this Order as part of the Sensitive Locations Data Program established and maintained pursuant to Provision III below.

Provided, however, that the prohibitions in this Provision II do not apply if Respondents: (i) use Sensitive Location Data to convert such data into data that (a) is not Sensitive Location Data or (b) is not Location Data; or (ii) have a direct relationship with the consumer related to the Sensitive Location Data, the consumer has provided Affirmative Express Consent, and the Sensitive Location Data is used to provide a service directly requested by the consumer.

III. Sensitive Location Data Program

IT IS FURTHER ORDERED that Respondents, within 90 days of the effective date of this Order, must establish and implement, and thereafter maintain, a Sensitive Location Data Program to develop a comprehensive list of Sensitive Locations and to prevent the use, sale, licensing, transfer, sharing, or disclosure of Sensitive Location Data as provided in Provision II above. To satisfy this requirement, Respondents must, at a minimum:

A. Document in writing the components of the Sensitive Location Data Program as well as the plan for implementing and maintaining the Sensitive Location Data Program;

B. Identify a senior officer, such as a Chief Privacy Officer or Chief Compliance Officer, to be responsible for the Sensitive Location Data Program. The senior officer will be approved by and report directly to the board of directors or a committee thereof or, if no such board or equivalent body exists, to the principal executive officer of Respondents;

C. Provide the written program and any evaluations thereof or updates thereto to Respondents' board of directors or governing body or, if no such board or equivalent body exists, to the principal executive officer of Respondents at least every twelve months;

D. Develop and implement procedures to identify Sensitive Locations to be used by Respondents in preventing the sale, license, transfer, use, or other sharing or disclosure of Sensitive Location Data as provided in Provision II above. If a building or place is identified as including both a Sensitive Location and a non-Sensitive Location, Respondents may associate Location Data with the non-Sensitive Location only;

E. Assess, update, and document, at least once every three months, the accuracy and completeness of Respondents' list of Sensitive Locations. Respondents' assessments must include:

    1. Verifying that Respondents' list includes Sensitive Locations known to Respondents;

    2. Identifying and assessing methods, sources, products, and services developed by Respondents or offered by third parties that identify Sensitive Locations;

    3. Updating its list of Sensitive Locations by selecting and using the methods, sources, products, or services developed by Respondents or offered by third parties that are accurate and comprehensive in identifying Sensitive Locations;

    4. Considering new categories of Sensitive Locations, not enumerated in the definition of Sensitive Locations, such as those based on an announcement by a self-regulatory association. Respondents must determine whether to add the newly identified categories to Respondents' list of Sensitive Locations and, as applicable, complete these additions within the time frames specified in Section III.G; and

5. Documenting each step of this assessment, including the reasons Respondents selected the methods, sources, products, or services used in updating Respondents' list of Sensitive Locations.

F. Implement policies, procedures, and technical measures designed to prevent Respondents from using, selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data as provided in Provision II above, and monitor and test the effectiveness of these policies, procedures, and technical measures at least once every three months. Such testing must be designed to verify that Respondents are not using, selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data;

G. Initiate the process of deleting or rendering non-sensitive Sensitive Location Data associated with locations included in the list developed pursuant to Subparts D and E, within 2 days of adding the location to the list of Sensitive Locations, and complete the process within 30 days of initiation, except where retention is needed to fulfill an allowed purpose as provided in Provision II above. The time period to complete this process may be extended by additional 30 days periods (not to exceed 90 total days) when reasonably necessary, provided the Respondents document at each interval, the reasons for the extension and the progress made, and Respondents must not use, provide access to, or disclose Sensitive Location Data during the process of deleting or rendering non-sensitive, for any other purpose; and

H. Evaluate and adjust the Sensitive Location Data Program in light of any changes to Respondents' operations or business arrangements, or any other circumstance that Respondents know or have reason to know may have an impact on the Sensitive Location Data Program's effectiveness. At a minimum, Respondents must evaluate the Sensitive Location Data Program every twelve months and implement modifications based on the results.

IV. Other Location Data Obligations

IT IS FURTHER ORDERED that Respondents, within 90 days of the effective date of this Order, must establish and implement and thereafter maintain policies, procedures, and technical measures designed to prevent Respondents or recipients of Respondents' Location Data, for any such Location Data received after the effective date of this Order, from (i) associating such data with (a) locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars, and nightlife, or (b) locations of public gatherings of individuals during political or social demonstrations, marches, and protests; or (ii) using such Location Data to determine the identity or the location of an individual's home, i.e., the location of any individual's private residences (e.g., single family homes, apartments, condominiums, townhomes) (together, "Prohibited Uses").

Respondents must identify a senior officer, such as a Chief Privacy Officer or Chief Compliance Officer, to be responsible for these policies, procedures, and technical measures. With respect to recipients of Respondents' Location Data, such policies, procedures, and technical measures shall include:

1. Contractual prohibitions against recipients of Respondents' Location Data from using Respondents' Location Data in whole or in part to associate a specific individual with the locations identified above, and contractual obligations on recipients of Respondents' Location Data requiring such recipients to impose equivalent prohibitions on any third parties to whom the recipient resells, transfers, or discloses Respondent's Location Data in its Raw Format;

   Provided, however, reselling does not include a recipient receiving Location Data on behalf of a designated end user, for which end user Respondents have implemented policies, procedures, and technical measures required by this Provision IV, and the end user has (a) contractually agreed to the prohibitions against reselling; and (b) contractually agreed not to engage in Prohibited Uses;

2. Marking techniques, such as seeding or salting, designed to detect recipients' non-compliance with any contractual prohibitions against resale or re-license of Respondents' Location Data;

3. Assessing and documenting recipients' compliance at least once every twelve months for as long as the recipient retains a copy of Respondents' Location Data; and

4. Terminating relationships with recipients for non-compliance.

V. Third-Party Incident Reports

IT IS FURTHER ORDERED that within 30 days of any Respondent's determination that a Third-Party Incident has occurred, Respondents must submit a report to the Commission. The report must include, to the extent possible:

A. The estimated date range when the Third-Party Incident occurred;

B. A description of the facts relating to the Third-Party Incident, including the causes of the Third-Party Incident, if known, and participants;

C. A description of each type of information that was affected by the Third-Party Incident;

D. The numbers of consumers whose information was affected by the Third-Party Incident;

E. The acts Respondents has taken to date to remediate the Third-Party Incident and protect Covered Information from further exposure or access; and

F. Unless otherwise directed by a Commission representative in writing, Respondents must submit all Third-Party Incident reports to the Commission under penalty of perjury as specified in the Section of this Order titled "Compliance Report and Notices."

VI. Limitations on Collection, Use, Maintenance, and Disclosure of Location Data

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must not:

A. Collect, use, maintain, or disclose Location Data from devices where a consumer has enabled the mobile operating system privacy settings to opt out of, limit, or otherwise decline targeted advertising or tracking, without a record satisfying the requirements in Provision VII.B, documenting the consumer's consent.

B. Within 90 days of the effective date of this Order, collect, use, maintain, or disclose an individual's Location Data without a record satisfying the requirements in Provision VII.B, documenting the consumer's consent obtained prior to Respondents' collection or use of Location Data.

VII. Supplier Assessment Program

IT IS FURTHER ORDERED that Respondents, within 90 days of the effective date of this Order, must implement a program designed to ensure that consumers have provided consent for the collection and use of all data that may reveal a mobile device or consumer's precise location, obtained by Respondents, including by implementing and maintaining a "Supplier Assessment Program." In connection with the Supplier Assessment Program, Respondents must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Supplier Assessment Program;

B. Conduct an initial assessment either within 30 days of a third party entering into data sharing agreements with Respondents (or, for parties with existing data-sharing agreements, within 30 days of the effective date of this Order) or within 30 days of the initial date of data collection from such a third party, and thereafter annually, designed to confirm that consumers provide Affirmative Express Consent if feasible or to confirm that consumers specifically consent to the collection, use, and disclosure of all data that may reveal a mobile device or a consumer's precise location;

C. Create and maintain records of the suppliers' responses obtained by Respondents under the Supplier Assessment Program; and

D. Cease from using, selling, licensing, transferring, or otherwise sharing or disclosing all data that may reveal a mobile device or consumer's precise location for which consumers have not provided consent, as provided in Provision VII.B above.

VIII. Disclosures to Consumers

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must provide a Clear and

Conspicuous means for consumers to request the identity of any entity, business, or individual as to which Respondents have knowledge that consumers' Location Data was sold, transferred, licensed, or otherwise disclosed. Respondents may require consumers to provide Respondents with information reasonably necessary to complete such requests and to verify their identity, but must not use, provide access to, or disclose any information collected for such a request for any other purpose.

Provided however, that the Disclosure requirements in this Provision VIII do not apply if Respondents provide consumers with a Clear and Conspicuous method to submit a request to delete their Location Data from the commercial databases of all recipients of such Location Data, expressly instruct (or contractually require) such recipients to honor such requests sent or made available to them by Respondents, expressly request (or contractually demand) written confirmation of deletion of the identified Location Data, and provide consumers with written confirmation of such deletion requests or instructions sent to recipients and written confirmation of deletion from recipients (where confirmed), no later than 90 days after the receipt of consumers' requests. Respondents may require consumers to provide Respondents with information reasonably necessary to complete such requests and to verify their identity, but must not use, provide access to, or disclose any information collected for such a request for any other purpose.

IX. Withdrawing Consent

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them who receive actual notice of this Order, whether acting directly or indirectly, must provide a simple, easily-located means for consumers to withdraw consent to Respondents' use or disclosure of their device's Location Data. Such means may include a Clear and Conspicuous notice or link to an applicable operating system or device setting. Respondents may require consumers to provide Respondents with information necessary to complete such requests, but Respondents must not use, provide access to, or disclose any information collected for such a request for any other purpose.

X. Obligations When Consent is Withdrawn

IT IS FURTHER ORDERED that Respondents, and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must cease using and disclosing all Location Data associated with a specific device within 15 days after Respondents receive notice that the consumer has withdrawn their consent through the means required by Provision IX.

XI. Location Data Deletion Requests

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must implement and maintain a simple and Clear and Conspicuous means for consumers to request that Respondents delete

Location Data that Respondents previously collected about their mobile device, and delete such Location Data within 30 days of receipt of such request unless a shorter period for deletion is required by law. Respondents shall create and maintain a process by which a deletion request provided to one Respondent is treated as notice to both Respondents. Respondents may require consumers to provide Respondents with information necessary to complete such requests, but must not use, provide access to, or disclose any information collected for a deletion request for any other purpose.

XII. Data Retention Limits

IT IS FURTHER ORDERED that Respondents, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must:

A. Within 60 days of the effective date of this Order, document, adhere to, and make publicly available through a link on the home page of their website(s), in a manner that is Clear and Conspicuous, a retention schedule for Covered Information, setting forth: (1) the purpose or purposes for which each type of Covered Information is collected or used; (2) the specific business needs for retaining each type of Covered Information; and (3) an established timeframe for deletion of each type of Covered Information limited to the time reasonably necessary to fulfill the purpose for which the Covered Information was collected, and in no instance providing for the indefinite retention of any Covered Information;

B. Within 60 days of the effective date of this Order, Respondents shall provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, describing the retention schedule for Covered Information made publicly available on its website(s); and

C. Prior to collecting or using any new type of information related to consumers that was not being collected as of the issuance date of this Order, and is not described in retention schedules published in accordance with sub-Provision A of this Provision entitled Data Retention Limits, Respondents must update its retention schedule setting forth: (1) the purpose or purposes for which the new information is collected; (2) the specific business needs for retaining the new information; and (3) a set timeframe for deletion of the new information that precludes indefinite retention.

XIII. Deletion

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must, unless prohibited by law:

A. Within 60 days after the effective date of this Order, delete or destroy all Historic Location Data, and provide a written statement to the Commission, pursuant to Provision XVI.D, confirming that all such information has been deleted or destroyed;

B. Within 90 days after the effective date of this Order, (i) inform Respondents' customers that received Historic Location Data within 3 years prior to the issuance date of this Order, of the FTC's requirement in Provision XIII.A that the FTC requires such data to be deleted, Deidentified, or rendered non-sensitive, and (ii) Respondents shall promptly submit, within 10 days of sending to its customers, all such notices to the Commission under penalty of perjury as specified in the Provision of this Order titled "Compliance Report and Notices"; and

C. Within 90 days after the effective date of this Order, delete or destroy all Data Products, and provide a written statement to the Commission, pursuant to Provision XVI.D, confirming such deletion or destruction.

Provided however, Respondents shall have the option to retain Historic Location Data and related Data Products if Respondents have obtained records in accordance with Provision VII showing that consumers consented to the collection, use, and disclosure of their Historic Location Data within 90 days after the effective date of this Order, or if within such time period Respondents ensure such Historic Location Data and Data Product is Deidentified or rendered non-sensitive in accordance with Provision III, and provided that the Historic Location Data and Data Product is subject to the obligations in Provision IV.

XIV. Mandated Privacy Program

IT IS FURTHER ORDERED that Respondents, and any business that Respondents control directly or indirectly, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within 60 days of the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive privacy program (the "Program") that protects the privacy of such Covered Information. To satisfy this requirement, Respondents must at a minimum do the following:

A. Document in writing the content, implementation, and maintenance of the Program;

B. Provide the written program, and any evaluations thereof or updates thereto to Respondents' board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondents responsible for the Program at least once every 12 months;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least once every 12 months, internal and external risks to the privacy of Covered Information that could result in the unauthorized collection, maintenance, use, disclosure of, or provision of access to Covered Information.

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondents identify to the privacy of Covered Information identified in response to Provision XIV.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk

could be realized and result in the unauthorized collection, maintenance, use, disclosure of, or provision of access to Covered Information.

F. On at least an annual basis, provide privacy training programs for all employees and independent contractors responsible for handling or who have access to Covered Information, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;

G. Test and monitor the effectiveness of the safeguards at least once every 12 months, and modify the Program based on the results; and

H. Evaluate and adjust the Program in light of any changes to Respondents' operations or business arrangements, new or more efficient technological or operational methods to control for the risks identified in Provision XIV.D of this Order, or any other circumstances that Respondents know or have reason to believe may have an impact on the effectiveness of the Program or any of their individual safeguards. At a minimum, Respondents must evaluate the Program at least once every 12 months and modify the Program based on the results.

XV. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

A. Respondents, within 10 days after the effective date of this Order, must submit to the Commission acknowledgments of receipt of this Order sworn under penalty of perjury.

B. For 5 years after the issuance date of this Order, Respondents must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of this Order, and all agents and representatives having managerial responsibilities for the conduct related to the subject matter of this Order; and (3) any business entity resulting from any change in structure as set forth in Provision XVI titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondents delivered a copy of this Order, Respondents must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

XVI. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

A. One year after the issuance date of this Order, each of the Respondents must submit a compliance report, sworn under penalty of perjury, in which the Respondents must:

(1) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondents; (2) identify all of the Respondents' businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (4) describe in detail whether and how the Respondents are in compliance with each Provision of this Order, including a discussion of all of the changes the Respondents made to comply with the Order; and (5) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. The Respondents must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (1) any designated point of contact; or (2) the structure of the Respondents or any entity that Respondents have any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. The Respondents must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against either Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: In re Gravy Analytics, Inc. & Venntel, Inc., FTC File No. 212-3035.

XVII. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for 5 years after the issuance date of the Order, and retain each such record for 5 years. Specifically, Respondents must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies of all consumer complaints that relate to the collection, use, maintenance, or disclosure of Covered Information, whether received directly or indirectly, such as through a third party, and any response;

D. For 5 years from the date received, copies of communications from law enforcement, if such communications request information or documents relating to Respondents' compliance with this Order;

E. A copy of each widely disseminated representation by either of the Respondents that describes the extent to which Respondents (i) review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt-in controls; (ii) the extent to which Respondents collect, use, maintain, disclose, or delete any Covered Information; and (iii) the extent to which the Location Data that Respondents collect, use, maintain, or disclose is Deidentified;

F. Records showing that Respondents have met the consent requirements set forth in Provision XIII for retaining Historic Location Data;

G. Records showing the Respondents' implementation of Supplier Assessment Program required by Provision VII;

H. Records showing Respondents' implementation of the Sensitive Location Data Program required by Provision III;

I. Records showing Respondents' processing of consumer deletion requests as provided in Provision VIII; and

J. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

XVIII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents' compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, the Respondents must submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondents. Respondents must permit representatives of the Commission to interview anyone affiliated with Respondents who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of

identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIX. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondents that are not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondents did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: January 13, 2025

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

January 13, 2025

National Partnership for Women & Families
c/o Ashley Emery
Senior Policy Analyst for Reproductive Health and Rights
aemery@nationalpartnership.org

Re: Gravy Analytics, Inc. and Venntel, Inc., FTC File No. 212-3035

Dear Ms. Emery:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement in the above-referenced proceeding against Gravy Analytics, Inc. ("Gravy") and Venntel, Inc. ("Venntel," and collectively with Gravy, the "Respondents"). The Commission has placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission is committed to protecting consumers from deceptive, unfair, and other unlawful practices, and we appreciate your feedback on this matter.

According to our complaint against Gravy and Venntel, Respondents violated the FTC Act by engaging in unfair practices relating to the collection, use, and retention of consumers' location data. The proposed order, among other robust obligations, bans Gravy and Venntel from disclosing or using sensitive location data as defined in the order in any products or services and to implement a sensitive location data program to prevent the use, sale, license, transfer, or sharing of sensitive location data. The order also requires Gravy and Venntel to implement a program designed to ensure that consumers have provided consent for the collection and use of location data obtained by the Respondents.

In your comment, you commend the Commission for this enforcement action and express support for the proposed consent agreement's prohibition on the sale of sensitive location data, including data collected from consumers visiting medical facilities. National Partnership particularly notes the risks that consumers face when information concerning consumers' use of abortion-related care and other sensitive health data is collected and sold in an unfair manner, including to law enforcement agencies. You also express support for the proposed consent agreement's requirement that Respondents delete historic location data and any data products using this data. We appreciate National Partnership's support of the proposed consent agreement. The Commission will continue to use its unfairness authority when appropriate to protect consumers' privacy and continue to require privacy-protective practices in our future enforcement work.

Additionally, your comment observes that the FTC must monitor compliance and enforce penalties for violations of the proposed consent order. The Commission appreciates National

Partnership's note about the importance of monitoring compliance and enforcing the Commission's orders. Provisions XV to XVIII of the proposed consent agreement contain mechanisms to monitor Respondents' compliance with the proposed consent agreement and facilitate the Commission's enforcement of the proposed consent agreement.

Having considered all the facts of this case and the comments submitted in response to the consent agreement, the Commission has now determined that the public interest would best be served by issuing the Complaint and the Decision and Order in the above-referenced proceeding in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at https://www.ftc.gov. It helps the Commission's analysis to hear from a variety of sources in its work, and it thanks you again for your comment.

By direction of the Commission.

April J. Tabor
Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

January 13, 2025

Hamlet Garcia, Jr.
The Catalyst Accord Central Office of Reform and Efficiency
101 E. Olney Ave, Unit 330
Philadelphia, PA 19120-3805

Re: Gravy Analytics, Inc. and Venntel, Inc., FTC File No. 212-3035

Dear Mr. Garcia:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement in the above-referenced proceeding against Gravy Analytics, Inc. ("Gravy") and Venntel, Inc. ("Venntel," and collectively with Gravy, the "Respondents"). The Commission has placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission is committed to protecting consumers from deceptive, unfair, and other unlawful practices, and we appreciate your feedback on this matter.

According to our complaint against Gravy and Venntel, Respondents violated the FTC Act by engaging in unfair practices relating to the collection, use, and retention of consumers' location data. The proposed order, among other robust obligations, bans Gravy and Venntel from disclosing or using sensitive location data as defined in the order in any products or services and to implement a sensitive location data program to prevent the use, sale, license, transfer, or sharing of sensitive location data. The order also requires Gravy and Venntel to implement a program designed to ensure that consumers have provided consent for the collection and use of location data obtained by the Respondents.

In your comment, you express concern that the order penalizes practices without actual injury, and thereby risks facilitating absurd results by penalizing lawful conduct, exceeds statutory boundaries, and fails to articulate clear and enforceable legal standards. You also assert that "vagueness in defining 'sensitive data,' 'misuse,' or 'potential harms'" conflicts with legal precedent requiring agency rules to provide clear notice of prohibited conduct.

With regard to your first concern, the Commission has long asserted that location data is sensitive data and that consumers are harmed when this data is collected or shared without consumers' informed consent.[1] The Commission continues to have significant privacy concerns

---

1 (Mar. 2012) at 6, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly*

around the practices of the geolocation data broker industry and will continue to use all our tools to protect Americans from deceptive or unfair practices in the industry. As described above, the proposed order addresses Respondents' unfair practices alleged in the Commission's proposed complaint, which include selling, licensing, or transferring precise location data associated with unique persistent identifiers that reveal consumers' visits to sensitive locations; failing to take reasonable steps to confirm consumers' consent for the collection, use, and sale of consumers' precise location data; and selling sensitive inferences about (and linked to) consumers, which are derived from consumers' precise location data.

As alleged in the complaint, millions of consumers suffered concrete and particularized injuries because of these practices. Specifically, consumers suffered an unwarranted invasion of privacy and were put at a significant risk of suffering secondary harms, including stigma, discrimination, physical violence, emotional distress, and other harms. Such harms are legally cognizable injuries and thus satisfy the requirements of Section 5 of the FTC Act. *See FTC v. Kochava*, No. 2:22-cv-00377, 2024 WL 449363 (D. Idaho Feb. 3, 2024). Accordingly, the proposed order is squarely within the Commission's statutory authority.

With regard to CORE's second concern, the proposed order defines "Sensitive Location Data" and "Sensitive Locations" similar to other Commission actions and settlements.[2] The Commission believes that these definitions are in line with the law and industry practices.

Having considered all the facts of this case and the comments submitted in response to the consent agreement, the Commission has now determined that the public interest would best be served by issuing the Complaint and the Decision and Order in the above-referenced proceeding in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at https://www.ftc.gov. It helps the Commission's analysis to hear from a variety of sources in its work, and it thanks you again for your comment.

By direction of the Commission.

April J. Tabor
Secretary

sensitive data (Jul. 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[2] *See In the Matter of X-Mode Social, Inc. and Outlogic, LLC*, No. C-4802 (F.T.C. Apr. 11, 2024); *In the Matter of InMarket Media, LLC*, No. C-4803 (F.T.C. Apr. 29, 2024).