**Analysis of Proposed Consent Order to Aid Public Comment**
***In the Matter of Gravy Analytics, Inc. and Venntel, Inc.*, File No. 2123035**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Gravy Analytics, Inc. ("Gravy Analytics") and Venntel, Inc. ("Venntel," and collectively with Gravy Analytics, "Respondents").

The proposed consent order ("Proposed Order") has been placed on the public record for 30 days for receipt of public comments by interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement, along with the comments received, and will decide whether it should make final the Proposed Order or withdraw from the agreement and take appropriate action.

Gravy Analytics and Venntel are Delaware corporations with their headquarters in Virginia. Respondent Venntel is a subsidiary of Gravy Analytics. Gravy Analytics and Venntel are data brokers that collect and sell precise geolocation data about consumers' mobile devices.

Gravy Analytics does not collect data directly from consumers. Rather, it purchases precise geolocation data and other personal data for its products from other data suppliers, including other data aggregators. Gravy Analytics offers several data products to its customers. These products include transfers of batch location data, consisting of a unique persistent identifier for the mobile device called a Mobile Advertiser ID ("MAID") and timestamped latitude and longitude coordinates; audience segments, which are groupings of MAIDs that purportedly share similar traits based on the locations or events the mobile devices and MAIDs have visited; and an online application programming interface that, among other things, enables Gravy Analytics' customers to geofence locations. Gravy Analytics makes its data products available to commercial customers, such as marketers, other data brokers, stores, and other commercial entities.

Venntel obtains mobile location data from Gravy Analytics exclusively. Venntel offers batch transfers of location data and allows customers to geofence specific locations. Venntel also offers its customers access to an online application programming interface through which its customers may search for devices that visited specific locations, obtain device information about a particular mobile phone, or obtain location data for individual devices. Venntel sells its data products only to public sector customers, such as government contractors.

The Commission's proposed three-count complaint alleges that Respondents violated Section 5(a) of the FTC Act by (1) unfairly selling sensitive location data and (2) unfairly collecting, using, and transferring consumer location data without consent verification; and that Gravy Analytics violated Section 5 of the FTC Act by (3) unfairly selling inferences about consumers' sensitive characteristics derived from location data.

With respect to the first count, the proposed complaint alleges that Respondents sold location data associated with persistent identifiers, such as MAIDs, that could be used to track consumers to sensitive locations, such as medical facilities, places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, and welfare and homeless shelters. For example, by plotting timestamped latitude and longitude coordinates

associated with mobile devices using publicly available map programs, it is possible to identify which consumers' mobile devices visited medical facilities and when.

With respect to the second count, the proposed complaint alleges that Respondents failed to verify that their data suppliers obtained informed consent from consumers to have the consumers' location data collected, used, and sold. Respondents' primary mechanism for ensuring that consumers have provided appropriate consent is through contractual requirements with their suppliers. However, contractual provisions, without additional safeguards, are insufficient to protect consumers' privacy.

With respect to the third count, the proposed complaint alleges that it was an unfair practice for Gravy Analytics to sell inferences about consumers' sensitive characteristics derived from their location data. Gravy Analytics created custom audience segments for customers based, for example, on consumers' attendance at a cancer charity run and based on consumers' church attendance, and has also offered standard audience segments based on medical decisions and political activities.

The proposed complaint alleges that Respondents could have addressed each of these failures by implementing certain safeguards at a reasonable cost and expenditure of resources.

The proposed complaint alleges that Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. Such practices constitute unfair acts or practices under Section 5 of the FTC Act.

**Summary of Proposed Order with Respondents**

The Proposed Order contains injunctive relief designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

**Part I** prohibits Respondents from misrepresenting the extent to which: (1) Respondents review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt in controls; (2) Respondents collect, maintain, use, disclose, or delete any covered information, and (3) the location data that Respondents collect, use, maintain, or disclose is deidentified.

**Part II** prohibits Respondents from selling, licensing, transferring, sharing, disclosing, or using sensitive location data in any products or services.

Sensitive locations are defined as those locations in 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.

This prohibition does not apply to sensitive location data used to respond to or prevent data security incidents, for national security purposes conducted by federal agencies or other federal entities, or for response by a federal law enforcement agency to an imminent risk of death or serious bodily harm to a person.

**Part III** requires that Respondents implement and maintain a sensitive location data program to develop a comprehensive list of sensitive locations and to prevent the use, sale, license, transfer, sharing, or disclosure of sensitive location data.

**Part IV** requires that Respondents establish and implement policies, procedures, and technical measures designed to prevent recipients of Respondents' location data from associating consumers with locations predominantly providing services to LGBTQ+ individuals, locations of public gatherings of individuals during social demonstrations, marches, or protests, or using location data to determine the identity or location of an individual's home.

**Part V** requires that Respondents notify the Commission any time Respondents determine that a third party shared Respondents' location data, in violation of a contractual requirement between Respondents and the third party.

**Part VI** requires that Respondents must not collect, use, maintain, and disclose location data: (1) when consumers have opted-out, or otherwise declined targeted advertising and (2) without a record documenting the consumer's consent obtained prior to the collection of location data.

**Part VII** requires that Respondents implement a supplier assessment program designed to ensure that consumers have provided consent for the collection and use of all data obtained by Respondents that may reveal a consumer's precise location. Under this program, Respondents must conduct initial assessments of all their data suppliers within 30 days of entering into a data sharing agreement, or within 30 days of the initial date of data collection. The program also requires that Respondents confirm that consumers provided consent and create and maintain records of suppliers' assessment responses. Finally, Respondents must cease from using, selling, or disclosing location data for which consumers have not provided consent.

**Part VIII** requires that Respondents provide a clear and conspicuous means for consumers to request the identity of any entity, business, or individual to whom Respondents know their location data has been sold, transferred, licensed, or otherwise disclosed or a method to delete the consumers' location data from the databases of Respondents' customers. Respondents must also provide written confirmation to consumers that the deletion requests have been sent to Respondents' customers.

**Part IX** requires that Respondents provide a simple, easily-located means for consumers to withdraw any consent provided and **Part X** requires that Respondents cease collecting

location data within 15 days after Respondents receive notice that the consumer withdraws their consent.

**Part XI** also requires that Respondents provide a simple, easily-located means for consumers to request that Respondents delete location data that Respondents previously collected and to delete the location data within 30 days of receipt of such request unless a shorter period for deletion is required by law.

**Part XII** requires that Respondents: (1) document and adhere to a retention schedule for the covered information they collect from consumers, including the purposes for which they collect such information, the specific business needs, and an established timeframe for its deletion, and (2) prior to collecting or using any new type of information related to consumers that was not previously collected, and is not described in its retention schedule, Respondents must update their retention schedules.

**Part XIII** requires that Respondents delete or destroy all historic location data and all data products developed using this data. Respondents have the option to retain historic location data if they have records showing they obtained consent or if they ensure that the historic location data is deidentified or rendered non-sensitive. Respondents must inform all customers that received location data from Respondents within 3 years prior to the issuance date of this Order of the Commission's position that such data should be deleted, deidentified, or rendered non-sensitive.

**Part XIV** requires Respondents to establish and implement, and thereafter maintain, a comprehensive privacy program that protects the privacy of consumers' personal information.

**Parts XV-XVIII** are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance.

**Part XIX** states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the Proposed Order, and it is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify the Proposed Order's terms in any way.